FortiOS™ Handbook

VERSION 5.2.12

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Friday, December 08, 2017

FortiOS™ Handbook

TABLE OF CONTENTS

Chapter 1 - What's New for FortiOS 5.2 ..... **44**

New features in FortiOS 5.2.12 44
New features in FortiOS 5.2.9 45
New features in FortiOS 5.2.8 45
New features in FortiOS 5.2.5 46
New features in FortiOS 5.2.4 48
New features in FortiOS 5.2.3 50
Interfaces on some FortiGate models are set in one-arm sniffer mode by default 50
Merge FGT-20C-ADSL and FWF-20C-ADSL 50
Log Viewer Improvements 51
Add AeroScout Inter-operabiliy testing 51
Add "Last connection time" Column in FortiView > VPN 51
FSSO agent support OU in group filters 52
Certificate GUI improvements 52
Improvement to WAN optimization feature 52
Add FortiAP LED dark support 52
Allow user to change VDOM operation mode more easily 53
Split 40G ports on some FortiGate models 53
Allow admin user to start/defer file system check if FGT was not shutdown properly 53
Cloud Sandboxing 53
Add a tooltip to remind users to activate FortiCloud to enable FortiSandbox cloud 53
Add warn about factory default certificate 53
Deep Flow 54
New features in FortiOS 5.2.2 54
Add allocator API and counters to scanunit 54
Add tooltips for application categories 56
Add broadcast/multicast suppression for local bridge mode ssid on the FAP side 56
Add hardware switch feature and SPAN functionality to 30D, 60, and 90D. Move POE ports out of Internal switch to independent interfaces 56
Disable performance statistics Logging 57
Improvements to firmware upload GUI dialog 57
Reimplementation of the session list as a part of FortiView to improve functionality and usability 58
Add GUI option to control the TLS versions for web administration 58

Cloud Wifi Support ... 58
Merge FWF/FGT-60D-3G4G and FGR-60D ... 58
Add FAP-224D/222C/25D/214B/21D/24D/112D/223C/321C support ... 59
Add support for more than 32k FortiClient configuration distribution through EC-NAC ... 60
Add a warning when using deep SSL inspection mode on security policy and SSL profile pages ... 60
Improve FSSO group GUI ... 60
Add Log Rate stats to System Resources widget ... 61
Add a command to export logs on local disk to external USB ... 61
Improve FortiView performance and add System Events, Admin Logins, and VPN ... 61
Integrate vmtools for FortiGate VMWare platforms ... 61
New features in FortiOS 5.2.1 ... 63
Include bandwidth and setup rate statistics in the event log ... 63
Allow export of collected emails ... 64
Ssl-ssh-profile is no longer mandatory when utm profiles are enabled ... 64
Disallow multiple destination interfaces on an IPsec firewall policy ... 64
Add a new diag test command for fnbamd ... 64
Add deregister all option in diagnose endpoint control registration ... 65
Redirect kernel messages to non-console terminals ... 65
Add FortiExtender supported 3G/4G modem list ... 65
Add a new option for STP forwarding ... 65
Suppress probe response based on threshold in wireless controller vap ... 66
Move global antivirus service settings into profile-protocol-options ... 66
Add Ekahau Blink Protocol support and reorganization for station-locate ... 66
Implement diagnose command to test flash SSD ... 67
Online help improvements ... 67
Add iprope check trace in flow trace ... 67
Log id-fields reference improvements ... 67
Add diagnose debug admin error-log command ... 68
Improve hasync debug ... 68
Improve interface list and switch mode ... 70
Wizard improvement ... 70
Allow VIP with port forwarding to permit ICMP ... 70
Support captive portal for block notification page ... 70
Add diagnose log clear-kernel-state command ... 71
Apply new LDAP Tree Browser design to the User Wizard and User Group page ... 71
New Join and try requests to FortiCloud for low-end models ... 71
Top Features ... 72
Unified Policy Management ... 72
FortiView Dashboards ... 72
SSL Inspection ... 73
Web Filtering ... 73

Application Control 73
IPsec VPN Creation Wizard 73
Captive Portal 73
FortiAP Management 74
Flow-based Antivirus 74
FortiExtender Support 74
Using a Virtual WAN Link for Redundant Internet Connections 74
Internet Key Exchange (IKE) 74
SSL VPN Creation 75
On-Net Status for FortiClient Devices 75
System Features 76
FortiExtender Support 76
Using a Virtual WAN Link for Redundant Internet Connections 78
FortiGuard Services 81
Netflow v9.0 82
DHCP Server Configuration 83
Improvements to Aggregate/Redundant Interfaces 84
Link Layer Discovery Protocol 86
CPU and Memory Usage per VDOM 86
Custom Languages for Guest Management and SSL VPN Portals 87
Packet Capture Options for Admin Profiles 88
FortiCloud Modem List 88
SPAN Support for Hard-Switch Interfaces 88
Setting the Service and AC-name in PPOE PADI/PADO Negotiations 89
Disabling FortiExplorer, the USB MGMT Port, and the Serial Console 89
Port Kernel Profiling 90
Using a Second Destination IP (VRDST) 90
Session Rate Stats per VDOM 90
Disable Honoring the Don't-Fragment Flag 90
Disable Login Time Recording 91
Per-IP-Bandwidth-Usage Feature Removed 91
Modem Support 91
Usability Enhancements 92
FortiView Dashboards 92
FortiExplorer Setup Wizard Improvements 97
Interfaces List Improvements 98
Dragging Objects Between Policies in the Policy List 99
Cloning Table Objects 99
DHCP-related Improvements in the Web-based Manager 99
System Resources Widget 99
License Information Widget 100
USB Modem Widget 100

New Feature Settings Preset 101
Improved Banned User List Page 101
Replacement Message Improvements 101
Sorting and Filtering Support for the Virtual IP list 101
Web-based Manager Options for the FortiGate-30D 101
Firewall 102
Menu Simplification 102
Unified Policy Management 103
Importing LDAP Users for a Security Policy 104
Dynamic VIP According to DNS Translation 105
GTP Rate Limiting 105
Object UUID Support 106
Configuring the Class of Service Bit 106
Hairpinning for NAT64 and NAT46 107
Maximum Number of Available Virtual IPs Increased 107
Security Profiles 108
Menu and Options Simplification 108
SSL Inspection 114
Web Filtering 116
Application Control 119
Flow-based Antivirus 121
Intrusion Protection System (IPS) 122
Vulnerability Scanning Visibility 123
Removed IM Proxy Options from the CLI 123
Client Reputation 123
IPsec VPN 124
VPN Creation Wizard 124
Internet Key Exchange (IKE) 126
Dynamic IPsec Route Control 128
Default Lifetimes and Proposal Values 129
Prioritizing DH Group Configuration 129
IPv6 Support for IPsec Phase 2 130
IPsec VPN Support with the FortiController-5103B 131
SSL VPN 132
SSL VPN Configuration 132
ECDSA Local Certificates 132
Host Security Check Error Replacement Message 133
Authentication 134
Captive Portal 134
User Authentication via a POP3 Server 135
Limiting Guest User Accounts 135
Nested Group Search in LDAP Authentication 136

Password Length for User Authentication 136
Certificates for Policy Authentication 136
Authentication Blackouts 136
Single Sign-On for Guest Accounts 137
Managing Devices 138
On-Net Status for FortiClient Devices 138
Endpoint Licenses 138
URL Filter Lists in Endpoint Control 139
FortiGuard Categories Consistency with FortiClient 139
Default Device Groups 139
Device Detection for Traffic Not Flowing Through the FortiGate 139
Wireless Networking 140
FortiAP Management 140
Captive Portal for WiFi 142
New Wireless Health Charts 142
RADIUS Accounting 143
802.11ac and DARRP Support 143
Date Channel DTLS in Kernel 143
IPv6 144
IPv6 Address Ranges 144
TCP MSS Values 144
RSSO Support 144
FortiManager Connections 145
Geographical Database 145
High Availability 146
DHCP and PPPOE Support for Active-Passive Mode 146
VRRP Support 146
Trigger Failover 147
Synchronizing a GTP Tunnel over Physical Ports 147
IPv6 Management Interface Gateway 147
WAN Optimization, Web Cache, and Explicit Proxy 148
Explicit Proxy Policy Table - for explicit web proxy, explicit FTP proxy and WAN optimization policies 148
Distributing Explicit Web Proxy Traffic to Multiple CPU Cores 148
Proxy Header Control 149
Explicit Web Proxy SOCKS services support for TCP and UDP traffic 150
Preventing the explicit web proxy from changing source addresses 150
Explicit web proxy firewall address URL patterns 150
Advanced Routing 152
BGP Neighbor Groups 152
OSPF Fast Hello 152
BGP Conditional Advertising 153

Source and Destination IP-based Mode for ECMP 153
Policy Routes 153
Logging and Reporting 154
Traffic and UTM Logging Improvements 154
FortiGate Daily Security Report 154
GTP Logging Improvements 155
Flash-based Logging Disabled on Some Models 156
Accessing Policy-specific Logs from the Policy List 156
IPS Event Context Data in Log Messages 156
Sniffer Traffic Log 156
Selecting Sources for Reports 156
Threat Weight 157
Disk Usage Information in System Event Logs 157
Event Log Generated When a Crash Occurs 157
Displaying FortiFlow Names 157
Other New Features 158
SIP Traffic is Handled by the SIP ALG by Default 158
Changing the Header Name of Load Balanced HTTP/HTTPS Traffic 158
TOS and DSCP Support for Traffic Mapping 159
RFC List 160
Chapter 2 - Getting Started 161
Differences between Models 162
Features 162
Names 162
Menus 162
Installation 163
NAT/Route Mode vs Transparent Mode 163
Installing a FortiGate in NAT/Route Mode 163
Installing a FortiGate in Transparent Mode 168
Troubleshooting your FortiGate Installation 170
Using Port Pairing to Simplify Transparent Mode 172
Using the Web-Based Manager 174
Connecting to the web-based manager 174
Menus 177
Dashboards 178
Feature settings 193
Information tables 194
Text strings 195
Basic Administration 197
Registration 197
System Settings 197
Firmware 202

FortiGuard 210
FortiCloud 220
Administrators 222
Passwords 232
Configuration Backups 233
Next Steps 240
Best Practices 240
The FortiGate Cookbook 240
The Fortinet Video Library 240
The FortiOS Handbook 240
Chapter 3 - Advanced Routing 241
Advanced Static Routing 242
Routing concepts 242
Static routing tips 257
Policy routing 258
Transparent mode static routing 262
Static routing example 263
Advanced static routing example: ECMP failover and load balancing 271
Dynamic Routing Overview 279
What is dynamic routing? 279
Comparison of dynamic routing protocols 282
Choosing a routing protocol 287
Dynamic routing terminology 288
IPv6 in dynamic routing 293
Routing Information Protocol (RIP) 295
RIP background and concepts 295
Troubleshooting RIP 307
Simple RIP example 311
RIPng — RIP and IPv6 326
Border Gateway Protocol (BGP) 332
BGP background and concepts 332
Troubleshooting BGP 345
Dual-homed BGP example 350
Redistributing and blocking routes in BGP 363
Open Shortest Path First (OSPF) 371
OSPF Background and concepts 371
Troubleshooting OSPF 383
Basic OSPF example 385
Advanced inter-area OSPF example 397
Controlling redundant links by cost 408
Intermediate System to Intermediate System Protocol(IS-IS) 412
IS-IS background and concepts 412

How IS-IS works 413
Troubleshooting IS-IS 418
Simple IS-IS example 421
Network layout and assumptions 422
Expectations 423
CLI configuration 423
Verification 425
Troubleshooting 428
Chapter 4 - Authentication 429
Change log 429
Introduction to authentication 431
What is authentication? 431
Methods of authentication 431
Types of authentication 433
Single Sign-On authentication for users 436
User's view of authentication 437
FortiGate administrator's view of authentication 437
General authentication settings 438
Authentication servers 440
FortiAuthenticator servers 440
RADIUS servers 440
LDAP servers 445
TACACS+ servers 455
POP3 servers 456
SSO servers 456
RSA ACE (SecurID) servers 458
Users and user groups 463
Users 463
User groups 477
Managing Guest Access 483
Configuring guest user access 483
Guest access in a retail environment 485
Configuring authenticated access 489
Authentication timeout 489
Password policy 490
Authentication protocols 492
Authentication in Captive Portals 492
Authentication in security policies 492
Authentication replacement messages 493
VPN authentication 501
Captive portals 506
Introduction to Captive Portals 506

Configuring a captive portal 506
Customizing captive portal pages 508
Certificate-based authentication 514
What is a security certificate? 514
Certificates overview 515
Managing X.509 certificates 518
Configuring certificate-based authentication 526
Example — Generate a CSR on the FortiGate unit 528
Example — Generate and Import CA certificate with private key pair on OpenSSL 529
Example — Generate an SSL certificate in OpenSSL 530
Single Sign-On using a FortiAuthenticator unit 533
User's view of FortiAuthenticator SSO authentication 533
Administrator's view of FortiAuthenticator SSO authentication 533
Configuring the FortiAuthenticator unit 534
Configuring the FortiGate unit 534
Configuring the FortiClient SSO Mobility Agent 535
Viewing SSO authentication events on the FortiGate unit 536
Single Sign-On to Windows AD 537
Introduction to Single Sign-On with Windows AD 537
Configuring Single Sign On to Windows AD 537
FortiOS FSSO log messages 542
Testing FSSO 543
Troubleshooting FSSO 543
Agent-based FSSO 545
Introduction to agent-based FSSO 545
FSSO NTLM authentication support 551
Agent installation 554
Configuring the FSSO Collector agent for Windows AD 560
Configuring the FSSO TS agent for Citrix 571
Configuring FSSO with Novell networks 572
Configuring FSSO Advanced Settings 574
Configuring FSSO on FortiGate units 579
FortiOS FSSO log messages 585
Testing FSSO 586
Troubleshooting FSSO 587
SSO using RADIUS accounting records 589
User's view of RADIUS SSO authentication 589
Configuration Overview 589
Configuring the RADIUS server 589
Creating the FortiGate RADIUS SSO agent 590
Defining local user groups for RADIUS SSO 591
Creating security policies 592

Example: webfiltering for student and teacher accounts 593
Monitoring authenticated users 596
Monitoring firewall users 596
Monitoring SSL VPN users 596
Monitoring IPsec VPN users 597
Monitoring users Quarantine 597
Examples and Troubleshooting 599
Firewall authentication example 599
LDAP Dial-in using member-attribute example 605
RADIUS SSO example 607
Troubleshooting 614
Chapter 5 - Best Practices 616
Overview 616
General Considerations 616
Customer service and technical support 616
Fortinet Knowledge Base 616
System and performance 618
Performance 618
Shutting down 618
Migration 619
Information gathering 619
Object and policy migration 619
Testing and validation 619
Going live and obtaining feedback 620
Adding new services 620
Environmental specifications 621
Grounding 621
Rack mounting 621
Firmware 623
Firmware change management 623
Performing a firmware upgrade 626
Performing a firmware downgrade 627
Performing a configuration backup 627
Security Profiles (AV, Web Filtering etc.) 630
Firewall 630
Security 630
Authentication 631
Antivirus 631
Antispam 631
Intrusion Prevention System (IPS) 631
Email filter 632
URL filtering 632

Web filtering 633
Patch management 633
Policy configuration 633
Networking 635
Routing configuration 635
Advanced routing 635
Network Address Translation (NAT) 636
Transparent Mode 636
Using Virtual IPs (VIPs) 636
FGCP High Availability 637
Heartbeat interfaces 637
Interface monitoring (port monitoring) 638
WAN Optimization 639
Virtual Domains (VDOMs) 641
Per-VDOM resource settings 641
Virtual domains in NAT/Route mode 641
Virtual clustering 641
Explicit proxy 642
Wireless 643
Encryption and authentication 643
Geographic location 643
Network planning 643
Lowering the power level to reduce RF interference 644
Wireless client load balancing 644
Local bridging 644
Advertising SSIDs 645
Using static IPs in a CAPWAP configuration 645
Logging and reporting 646
Log management 646
System memory and hard disks 647
Chapter 6 - FortiOS Carrier 648
Overview of FortiOS Carrier features 649
Overview 649
Registering FortiOS Carrier 650
MMS background 650
How FortiOS Carrier processes MMS messages 654
MMS protection profiles 663
Bypassing MMS protection profile filtering based on carrier endpoints 664
Applying MMS protection profiles to MMS traffic 664
GTP basic concepts 664
GPRS network common interfaces 672
Packet flow through the GPRS network 673

SCTP 675
Carrier web-based manager settings 680
MMS Security features 727
Why scan MMS messages for viruses and malware? 727
MMS virus scanning 728
Sender notifications and logging 735
MMS content-based Antispam protection 738
MMS DLP archiving 740
Message flood protection 742
Overview 742
Setting message flood thresholds 743
Notifying administrators of floods 745
Example — three flood threshold levels with different actions for each threshold 745
Notifying message flood senders and receivers 748
Viewing DLP archived messages 749
Order of operations: flood checking before duplicate checking 749
Bypassing message flood protection based on user's carrier endpoints 750
Configuring message flood detection 750
Sending administrator alert notifications 751
Duplicate message protection 754
Overview 754
Using message fingerprints to identify duplicate messages 755
Messages from any sender to any recipient 756
Setting duplicate message thresholds 756
Duplicate message actions 756
Notifying duplicate message senders and receivers 757
Viewing DLP archived messages 759
Order of operations: flood checking before duplicate checking 759
Bypassing duplicate message detection based on user's carrier endpoints 759
Configuring duplicate message detection 759
Sending administrator alert notifications 759
Configuring GTP on FortiOS Carrier 762
GTP support on the Carrier-enabled FortiGate unit 762
Configuring General Settings on the Carrier-enabled FortiGate unit 764
Configuring Encapsulated Filtering in FortiOS Carrier 764
Configuring the Protocol Anomaly feature in FortiOS Carrier 766
Configuring Anti-overbilling in FortiOS Carrier 766
Logging events on the Carrier-enabled FortiGate unit 767
GTP message type filtering 769
Common message types on carrier networks 769
Configuring message type filtering in FortiOS Carrier 771
GTP identity filtering 777

IMSI on carrier networks 777
Other identity and location based information elements 777
Configuring APN filtering in FortiOS Carrier 780
Configuring IMSI filtering in FortiOS Carrier 781
Configuring advanced filtering in FortiOS Carrier 782
Troubleshooting 785
FortiOS Carrier diagnose commands 785
Applying IPS signatures to IP packets within GTP-U tunnels 787
GTP packets are not moving along your network 787
Chapter 7 - Compliance 792
Compliance 792
Introduction 792
Configuring FortiGate units for PCI DSS compliance 793
Chapter 8 - Deploying Wireless Networks 809
Introduction to wireless networking 810
Wireless concepts 810
Security 811
Authentication 813
Wireless networking equipment 813
Automatic Radio Resource Provisioning 814
Configuring a WiFi LAN 815
Overview of WiFi controller configuration 815
Setting your geographic location 817
Creating a FortiAP Profile 817
Defining a wireless network interface (SSID) 819
Dynamic VLAN assignment 828
Configuring user authentication 830
Configuring firewall policies for the SSID 832
Configuring the built-in access point on a FortiWiFi unit 833
Access point deployment 834
Overview 834
Network topology for managed APs 834
Discovering and authorizing APs 836
Advanced WiFi controller discovery 841
Wireless client load balancing for high-density deployments 842
LAN port options 844
Preventing IP fragmentation of packets in CAPWAP tunnels 846
Wireless Mesh 847
Overview of Wireless Mesh 847
Configuring a meshed WiFi network 851
Configuring a point-to-point bridge 853
Combining WiFi and wired networks with a software switch 855

Combining WiFi and wired networks with a software switch 855
FortiAP local bridging (Private Cloud-Managed AP) 857
Using bridged FortiAPs to increase scalability 860
Using Remote WLAN FortiAPs 861
Configuring the FortiGate for remote FortiAPs 861
Configuring the FortiAP units 862
Preauthorizing FortiAP units 863
Features for high-density deployments 863
Broadcast packet suppression 863
Multicast to unicast conversion 863
Ignore weak or distant clients 864
Turn off 802.11b protocol 864
Limit power 864
Use frequency band load-balancing 865
AP load balancing 865
Application rate-limiting 866
Protecting the WiFi Network 867
Wireless IDS 867
WiFi data channel encryption 868
Wireless network monitoring 870
Monitoring wireless clients 870
Monitoring rogue APs 870
Suppressing rogue APs 876
Monitoring wireless network health 876
Configuring wireless network clients 877
Windows XP client 877
Windows 7 client 882
Mac OS client 886
Linux client 888
Troubleshooting 890
Wireless network examples 893
Basic wireless network 893
A more complex example 898
Using a FortiWiFi unit as a client 909
Use of client mode 909
Configuring client mode 910
Support for location-based services 911
Overview 911
Configuring location tracking 911
Viewing device location data on the FortiGate unit 911
Reference 913
FortiAP web-based manager 914

Wireless radio channels 916
FortiAP CLI 917
Chapter 9 - Firewall 924
FortiGate Firewall Components 924
How does a FortiGate protect your network? 925
Firewall concepts 927
What is a firewall? 927
IPv6 930
NAT 938
How packets are handled by FortiOS 946
FortiGate modes 948
Quality of Service 948
Interfaces and zones 949
Firewall objects 951
UUID support 951
Addresses 951
Address groups 960
Virtual IPs 961
Virtual IP groups 964
IP pools 965
Services and TCP ports 968
Firewall schedules 999
Schedule groups 1001
Security policies 1003
Firewall policies 1003
Security profiles 1010
SSL/SSH inspection 1015
Identity-based policies 1021
VPN policies 1023
Interface policies 1023
DoS protection 1024
Local-In policies 1029
Security policy 0 1030
Deny policies 1031
Accept policies 1031
Fixed port 1031
Endpoint security 1031
Traffic logging 1032
Quality of service 1033
Policy Monitor 1034
Network defense 1036
Monitoring 1036

Blocking external probes 1036
Defending against DoS attacks 1041
GUI and CLI - what you may not know 1045
Mouse tricks 1046
Changing the default column setting on the policy page 1047
Naming rules and restrictions 1049
Character restrictions 1050
Numeric values 1051
Numeric values 1052
Selecting options from a list 1053
Enabling or disabling options 1054
To enable or disable optionally displayed features 1056
Building firewall objects and policies 1056
Building firewall objects and policies 1057
Example: IPv4 firewall addresses 1058
Example: IPv6 firewall addresses 1060
Example: FQDN address 1062
Changing the TTL of a FQDN address 1062
Example: Geography-based address 1063
Example: IPv4 address group 1063
Example: IPv6 address group 1064
Example: Multicast address 1065
Example: Service category 1066
Example: TCP/UDP/SCTP service 1067
Example: ICMP service 1069
Example: ICMPv6 service 1070
Example: Service group 1071
Example: Virtual IP address 1072
Example: IP pool 1074
Example: Central NAT table 1075
Example: Firewall schedule - recurring 1076
Example: Firewall schedule - one-time 1077
Example: Schedule group 1078
Example: Proxy option 1079
Example: DoS policy 1082
Multicast forwarding 1086
Sparse mode 1086
Dense mode 1087
Multicast IP addresses 1088
PIM Support 1088
Multicast forwarding and FortiGate units 1089
Configuring FortiGate multicast forwarding 1090

Multicast routing examples 1094
Chapter 10 - FortiView 1120
FortiView 1120
Overview 1121
FortiView consoles 1129
Reference 1136
Troubleshooting FortiView 1147
Chapter 11 - Hardening 1148
Hardening your FortiGate 1148
Install the FortiGate unit in a physically secure location 1148
Maintain the firmware 1148
Add new administrator accounts 1149
Change the admin account name and limit access to this account 1149
Only allow administrative access to the external interface when needed 1150
When enabling remote access, configure Trusted Hosts and Two-factor Authentication 1150
Change the default administrative port to a non-standard port 1151
Modify the device name 1151
Register with support services 1151
Maintain short login timeouts 1151
Enable automatic clock synchronization 1152
Enable Password Policy 1152
Modify administrator account Lockout Duration and Threshold values 1152
Disable auto installation via USB 1153
Configure auditing and logging 1153
Chapter 12 - Hardware Acceleration 1154
Hardware acceleration overview 1155
Content processors (CP4, CP5, CP6 and CP8) 1155
Security processors (SPs) 1157
Network processors (NP1, NP2, NP3, NP4 and NP6) 1160
Enabling strict protocol header checking disables all hardware acceleration 1165
sFlow and NetFlow and hardware acceleration 1165
Checking that traffic is offloaded by NP processors 1165
Controlling IPS NPx and CPx acceleration 1167
Dedicated Management CPU 1168
Offloading flow-based content inspection with NTurbo and IPSA 1168
NP6 Acceleration 1170
NP6 session fast path requirements 1170
NP6 processors and traffic shaping 1172
Viewing your FortiGate NP6 processor configuration 1172
Optimizing NP6 performance by distributing traffic to XAUI links 1173
Increasing NP6 offloading capacity using link aggregation groups (LAGs) 1175

Configuring Inter-VDOM link acceleration with NP6 processors 1175
Configuring individual NP6 processors 1178
Enabling per-session accounting for offloaded NP6 sessions 1184
FortiGate NP6 architectures 1185
FortiGate-300D fast path architecture 1185
FortiGate-400D fast path architecture 1185
FortiGate-500D fast path architecture 1186
FortiGate-600D fast path architecture 1187
FortiGate-800D fast path architecture 1188
FortiGate-900D fast path architecture 1190
FortiGate-1000D fast path architecture 1192
FortiGate-1200D fast path architecture 1194
FortiGate-1500D fast path architecture 1197
FortiGate-1500DT fast path architecture 1198
FortiGate-3000D fast path architecture 1200
FortiGate-3100D fast path architecture 1202
FortiGate-3200D fast path architecture 1203
FortiGate-3700D fast path architecture 1206
FortiGate-3700DX fast path architecture 1210
FortiGate-3810D fast path architecture 1214
FortiGate-3815D fast path architecture 1216
FortiGate-5001D fast path architecture 1217
FortiController-5902D fast path architecture 1219
NP4 Acceleration 1222
Viewing your FortiGate's NP4 configuration 1222
Configuring NP4 traffic offloading 1223
Increasing NP4 offloading capacity using link aggregation groups (LAGs) 1224
NP4 traffic shaping offloading 1225
NP4 IPsec VPN offloading 1225
NP4 IPsec VPN offloading configuration example 1226
Configuring Inter-VDOM link acceleration with NP4 processors 1230
Offloading NP4 anomaly detection 1234
FortiGate NP4 architectures 1237
FortiGate-600C 1237
FortiGate-800C 1238
FortiGate-1000C 1239
FortiGate-1240B 1240
FortiGate-3040B 1241
FortiGate-3140B 1242
FortiGate-3140B — load balance mode 1243
FortiGate-3240C 1243
FortiGate-3600C 1245

FortiGate-3950B and FortiGate-3951B 1246
FortiGate-3950B and FortiGate-3951B — load balance mode 1248
FortiGate-5001C 1249
FortiGate-5001B 1250
Setting switch-mode mapping on the ADM-XD4 1251
Hardware acceleration diagnose commands 1251
diagnose sys session/session6 list (IPv4, IP6, NAT46, NAT64, and IPsec session information) 1251
diagnose npu np6 session-stats <np6-id> (number of NP6 IPv4 and IPv6 sessions) 1255
diagnose npu np6 ipsec-stats (NP6 IPsec statistics) 1256
diagnose sys mcast-session/session6 list (IPv4 and IPv6 multicast sessions) 1257
diagnose npu np6 sse-stats <np6-id> (number of NP6 sessions and dropped sessions) 1258
diagnose npu np6 dce <np6-id> (number of dropped NP6 packets) 1258
diagnose hardware deviceinfo nic <interfac-name> (number of packets dropped by an interface) 1259
dianose npu np6 synproxy-stats (NP6 SYN-proxied sessions and unacknowledged SYNs) 1260
Chapter 13 - High Availability 1261
FortiOS 5.2 HA new features 1262
Solving the High Availability problem 1263
FortiGate Cluster Protocol (FGCP) 1263
FortiGate Session Life Support Protocol (FGSP) 1265
VRRP 1266
Fortinet redundant UTM protocol (FRUP) 1266
Session-Aware Load Balancing Clustering (SLBC) 1267
Enhanced Load Balancing Clustering (ELBC) 1268
Content clustering 1268
An introduction to the FGCP 1270
About the FGCP 1270
Synchronizing the configuration (and settings that are not synchronized) 1273
Preparing the FortiGates before setting up a FGCP cluster 1274
Configuring FortiGate units for FGCP HA operation 1275
Active-passive and active-active HA 1278
Identifying the cluster and cluster units 1279
Device failover, link failover, and session failover 1280
Primary unit selection 1280
HA override 1288
FortiGate HA compatibility with DHCP and PPPoE 1292
HA and distributed clustering 1293
Clusters of three or four FortiGate units 1293
Disk storage configuration and HA 1296
FGCP HA terminology 1298

HA web-based manager options 1302
FGCP high availability best practices 1304
FGCP HA terminology 1306
HA GUI options 1309
FGCP configuration examples and troubleshooting 1313
About the examples in this chapter 1313
How to set up FGCP clustering (recommended steps) 1313
Setting up two new FortiGates as an FGCP cluster 1319
Adding a new FortiGate to an operating cluster 1331
Active-active HA cluster in Transparent mode 1331
FortiGate-5000 active-active HA cluster with FortiClient licenses 1343
Converting a standalone FortiGate unit to a cluster 1353
Replacing a failed cluster unit 1358
FGCP HA with 802.3ad aggregated interfaces 1359
Example HA and redundant interfaces 1371
Troubleshooting HA clusters 1381
Virtual clusters 1387
Virtual clustering overview 1387
Configuring HA for virtual clustering 1389
Example virtual clustering with two VDOMs and VDOM partitioning 1391
Example inter-VDOM links in a virtual clustering configuration 1404
Troubleshooting virtual clustering 1406
Full mesh HA 1407
Full mesh HA overview 1407
Example full mesh HA configuration 1409
Troubleshooting full mesh HA 1419
Operating a cluster 1421
Operating a cluster 1421
Operating a virtual cluster 1421
Managing individual cluster units using a reserved management interface 1422
Managing individual cluster units in a virtual cluster 1426
The primary unit acts as a router for subordinate unit management traffic 1426
Clusters and FortiGuard services 1427
Clusters and logging 1428
Clusters and SNMP 1431
Adding FortiClient licenses to a cluster 1435
Cluster members list 1437
Virtual cluster members list 1438
Viewing HA statistics 1438
Changing the HA configuration of an operating cluster 1438
Changing the HA configuration of an operating virtual cluster 1439
Changing the subordinate unit host name and device priority 1439

Upgrading cluster firmware 1439
Downgrading cluster firmware 1441
Backing up and restoring the cluster configuration 1442
Monitoring cluster units for failover 1442
Viewing cluster status from the CLI 1443
Disconnecting a cluster unit from a cluster 1451
Adding a disconnected FortiGate unit back to its cluster 1452
HA diagnose commands 1453
HA and failover protection 1455
About active-passive failover 1455
About active-active failover 1456
Device failover 1456
HA heartbeat and communication between cluster units 1457
Cluster virtual MAC addresses 1464
Synchronizing the configuration 1471
Synchronizing kernel routing tables 1480
Configuring graceful restart for dynamic routing failover 1482
Synchronizing IPsec VPN SAs 1484
Link failover (port monitoring or interface monitoring) 1485
Subsecond failover 1491
Remote link failover 1491
Session failover (session pick-up) 1496
WAN optimization and HA 1501
Failover and attached network equipment 1501
Monitoring cluster units for failover 1502
NAT/Route mode active-passive cluster packet flow 1502
Transparent mode active-passive cluster packet flow 1504
Failover performance 1506
HA and load balancing 1509
Load balancing overview 1509
Selecting a load balancing schedule 1511
Load balancing TCP and UDP sessions 1512
Using NP4 or NP6 processors to offload load balancing 1512
Configuring weighted-round-robin weights 1512
Dynamically optimizing weighted load balancing according to how busy cluster units are 1514
NAT/Route mode active-active cluster packet flow 1517
Transparent mode active-active cluster packet flow 1520
HA with FortiGate-VM and third-party products 1524
FortiGate-VM for VMware HA configuration 1524
FortiGate VM for Hyper-V HA configuration 1524
Troubleshooting layer-2 switches 1525

Failover issues with layer-3 switches 1525
Changing spanning tree protocol settings for some switches 1525
Failover and attached network equipment 1526
Ethertype conflicts with third-party switches 1526
LACP, 802.3ad aggregation and third-party switches 1527
VRRP 1528
Configuring VRRP 1531
FortiGate Session Life Support Protocol (FGSP) 1535
Synchronizing the configuration 1537
Synchronizing UDP and ICMP (connectionless) sessions 1538
Synchronizing NAT sessions 1538
Synchronizing asymmetric sessions 1538
Synchronizing expectation sessions 1539
Security profile flow-based inspection and asymmetric traffic 1539
Notes and limitations 1540
Configuring FGSP HA 1540
Configuring the session synchronization link 1541
Basic example configuration 1541
Verifying FGSP configuration and synchronization 1544
Configuring FRUP 1546
FRUP and the mode of the FortiGate hardware switch 1546
FRUP configuration example 1547
Chapter 14 - IPsec VPN 1552
IPsec VPN concepts 1554
VPN tunnels 1554
VPN gateways 1555
Clients, servers, and peers 1557
Encryption 1557
Authentication 1558
Phase 1 and Phase 2 settings 1559
Security Association 1560
IKE and IPsec packet processing 1560
IPsec VPN overview 1563
Types of VPNs 1563
Planning your VPN 1565
General preparation steps 1566
How to use this guide to configure an IPsec VPN 1567
IPsec VPN in the web-based manager 1568
Phase 1 configuration 1568
Phase 2 configuration 1574
Concentrator 1580
IPsec Monitor 1580

Phase 1 parameters 1581
Overview 1581
Defining the tunnel ends 1582
Choosing Main mode or Aggressive mode 1582
Choosing the IKE version 1583
Authenticating the FortiGate unit 1583
Authenticating remote peers and clients 1586
Defining IKE negotiation parameters 1591
Using XAuth authentication 1595
Dynamic IPsec route control 1596
Phase 2 parameters 1598
Phase 2 settings 1598
Configuring the Phase 2 parameters 1600
Defining VPN security policies 1603
Defining policy addresses 1603
Defining VPN security policies 1604
Gateway-to-gateway configurations 1609
Configuration overview 1609
General configuration steps 1611
Configuring the two VPN peers 1611
How to work with overlapping subnets 1616
Testing 1620
Hub-and-spoke configurations 1623
Configuration overview 1623
Configure the hub 1625
Configure the spokes 1629
Dynamic spokes configuration example 1633
Dynamic DNS configuration 1639
Dynamic DNS over VPN concepts 1639
Dynamic DNS topology 1641
General configuration steps 1643
Configure the dynamically-addressed VPN peer 1643
Configure the fixed-address VPN peer 1648
Testing 1652
FortiClient dialup-client configurations 1654
Configuration overview 1654
FortiClient-to-FortiGate VPN configuration steps 1659
Configure the FortiGate unit 1659
Configure the FortiClient Endpoint Security application 1663
Adding XAuth authentication 1663
FortiClient dialup-client configuration example 1663
FortiGate dialup-client configurations 1669

Configuration overview 1669
FortiGate dialup-client configuration steps 1671
Configure the server to accept FortiGate dialup-client connections 1672
Configure the FortiGate dialup client 1674
Supporting IKE Mode config clients 1676
Automatic configuration overview 1676
IKE Mode Config overview 1676
Configuring IKE Mode Config 1676
Example FortiGate unit as IKE Mode Config server 1680
Example FortiGate unit as IKE Mode Config client 1680
Internet-browsing configuration 1682
Configuration overview 1682
Creating an Internet browsing security policy 1683
Routing all remote traffic through the VPN tunnel 1684
Redundant VPN configurations 1686
Configuration overview 1686
General configuration steps 1687
Configure the VPN peers - route-based VPN 1688
Redundant route-based VPN configuration example 1690
Partially-redundant route-based VPN example 1703
Creating a backup IPsec interface 1710
Transparent mode VPNs 1711
Configuration overview 1711
Configure the VPN peers 1715
IPv6 IPsec VPNs 1717
Overview of IPv6 IPsec support 1717
Configuring IPv6 IPsec VPNs 1718
Site-to-site IPv6 over IPv6 VPN example 1719
Site-to-site IPv4 over IPv6 VPN example 1723
Site-to-site IPv6 over IPv4 VPN example 1726
L2TP and IPsec (Microsoft VPN) 1730
Overview 1730
Assumptions 1731
Configuring the FortiGate unit 1731
Configuring the Windows PC 1736
Troubleshooting 1737
GRE over IPsec (Cisco VPN) 1741
Overview 1741
Configuring the FortiGate unit 1741
Configuring the Cisco router 1747
Troubleshooting 1747
Protecting OSPF with IPsec 1750

Overview 1750
OSPF over IPsec configuration 1750
Creating a redundant configuration 1756
Redundant OSPF routing over IPsec 1758
Creating redundant IPsec tunnels on FortiGate 1 1758
Configuring IP addresses and OSPF on FortiGate 1 1758
Configuring firewall addresses on FortiGate 1 1759
Configuring security policies on FortiGate 1 1759
Creating redundant IPsec tunnels on FortiGate 2 1759
Configuring IP addresses and OSPF on FortiGate 2 1760
Configuring firewall addresses on FortiGate 2 1760
Configuring security policies on FortiGate 2 1761
Results 1761
OSPF over dynamic IPsec 1762
Configuring IPsec on FortiGate 1 1762
Configuring OSPF on FortiGate 1 1762
Adding policies on FortiGate 1 1763
Configuring IPsec on FortiGate 2 1763
Configuring OSPF on FortiGate 2 1763
Adding policies on FortiGate 2 1764
Verifying the tunnel is up 1764
Results 1764
BGP over dynamic IPsec 1765
Configuring IPsec on FortiGate 1 1765
Configuring BGP on FortiGate 1 1766
Adding policies on FortiGate 1 1766
Configuring IPsec on FortiGate 2 1766
Configuring BGP on FortiGate 2 1767
Adding policies on FortiGate 2 1767
Adding a static route on FortiGate 2 1767
Verifying the tunnel is up 1767
Results 1767
Logging and monitoring 1769
Monitoring VPN connections 1769
Logging VPN events 1770
Troubleshooting 1771
VPN troubleshooting tips 1775
General troubleshooting tips 1776
Chapter 15 - IPv6 1778
Possible addresses: 1778
IPv6 packet structure 1779
Benefits of IPv6 1779

IPv6 Features ... 1780
IPv6 policies ... 1780
IPv6 Network Address Translation ... 1792
ICMPv6 ... 1798
IPv6 in dynamic routing ... 1803
Dual stack routing ... 1804
IPv6 tunnelling ... 1804
SIP over IPv6 ... 1805
New Fortinet FortiGate IPv6 MIB fields ... 1806
IPv6 Per-IP traffic shaper ... 1807
DHCPv6 ... 1808
IPv6 forwarding ... 1808
Obtaining IPv6 addresses from an IPv6 DHCP server ... 1808
IPv6 Configuration ... 1809
IPv6 address groups ... 1809
IPv6 address ranges ... 1810
IPv6 firewall addresses ... 1811
ICMPv6 ... 1813
IPv6 IPsec VPN ... 1813
TCP MSS values ... 1826
BGP and IPv6 ... 1826
RIPng — RIP and IPv6 ... 1827
IPv6 RSSO support ... 1833
IPv6 IPS ... 1833
Blocking IPv6 packets by extension headers ... 1833
IPv6 Denial of Service policies ... 1834
Configure hosts in an SNMP v1/2c community to send queries or receive traps ... 1834
IPv6 PIM sparse mode multicast routing ... 1834
Chapter 16 - Life of a Packet ... 1835
Life of a Packet ... 1835
Packet flow ... 1836
Comparison of inspection types ... 1843
Client/Server connection packet flow example ... 1845
Routing table update packet flow example ... 1847
Dialup IPsec VPN with Application control example ... 1848
Chapter 17 - Load Balancing ... 1850
Before you begin ... 1850
How this chapter is organized ... 1850
Configuring load balancing ... 1851
Load balancing and other FortiOS features ... 1852
Configuring load balancing from the web-based manager ... 1852
Configuring load balancing from the CLI ... 1854

Load balancing methods 1854
Session persistence 1856
Real servers 1856
Health check monitoring 1858
Load balancing limitations 1860
Monitoring load balancing 1860
Load balancing diagnose commands 1861
Basic load balancing configuration example 1863
HTTP and HTTPS load balancing, multiplexing, and persistence 1867
SSL/TLS load balancing 1871
IP, TCP, and UDP load balancing 1879
Load balancing configuration examples 1880
Example HTTP load balancing to three real web servers 1880
Example Basic IP load balancing configuration 1885
Example Adding a server load balance port forwarding virtual IP 1886
Example Weighted load balancing configuration 1888
Example HTTP and HTTPS persistence configuration 1891
Chapter 18 - Logging and Reporting 1896
Logging and reporting overview 1897
What is logging? 1897
FortiOS features available for logging 1898
Log messages 1903
Log files and types 1910
Log database and datasets 1911
Log devices 1913
Reports 1917
Best Practices: Log management 1919
Logging and reporting for small networks 1921
Modifying default log device settings 1921
Configuring the backup solution 1923
Modifying the default FortiOS report 1924
Logging and reporting for large networks 1925
Modifying default log device settings 1925
Configuring the backup solution 1927
Modifying the default FortiOS report 1929
Uploading the corporate images 1930
Advanced logging 1932
Configuring logging to multiple Syslog servers 1932
Using Automatic Discovery to connect to a FortiAnalyzer unit 1933
Activating a FortiCloud account for logging purposes 1933
Viewing log storage space 1934
Customizing and filtering log messages 1934

Viewing logs from the CLI 1935
Configuring NAC quarantine logging 1935
Logging local-in policies 1936
Tracking specific search phrases in reports 1939
Reverting modified report settings to default settings 1940
Troubleshooting and logging 1941
Using log messages to help in troubleshooting issues 1941
Connection issues between FortiGate unit and logging devices 1942
Log database issues 1942
Logging daemon (Miglogd) 1944
Chapter 19 - Managing Devices 1945
Managing “bring your own device” 1946
Device monitoring 1946
Device Groups 1947
Controlling access with a MAC Address Access Control List 1947
Security policies for devices 1948
Creating device policies 1949
Endpoint Protection 1951
Endpoint Protection overview 1951
Configuration overview 1953
Creating a FortiClient profile 1954
Creating the registration key 1956
Enabling Endpoint Protection in security policies 1956
Configuring endpoint registration over a VPN 1957
Monitoring endpoints 1958
Modifying the Endpoint Protection replacement messages 1958
Vulnerability Scan 1959
Configuring vulnerability scans 1959
Running a vulnerability scan and viewing scan results 1961
Requirements for authenticated scanning and ports scanned 1961
Microsoft Windows hosts - domain scanning 1961
Chapter 20 - Managing a FortiSwitch with a FortiGate 1968
Managing a FortiSwitch with a FortiGate 1968
Introduction 1968
Getting Started 1970
VLAN Configuration 1975
Port Configuration 1979
Scenarios 1980
Chapter 21 - Security Profiles 1999
Security Profiles overview 2000
Traffic inspection 2000
Content inspection and filtering 2001

Security Profiles components 2003
Security Profiles/lists/sensors 2004
AntiVirus 2006
Antivirus concepts 2006
Enabling AntiVirus scanning 2019
Testing your antivirus configuration 2021
Example Scenarios 2021
Web filter 2027
Web filter concepts 2027
Inspection Modes 2029
FortiGuard Web Filtering Service 2030
Overriding FortiGuard website categorization 2033
SafeSearch 2039
YouTube Education Filter 2040
Static URL Filter 2040
Web content filter 2045
Advanced web filter configurations 2048
Configuring Web Filter Profiles 2052
Web filtering example 2057
Application control 2061
Application control concepts 2061
Application Control Actions 2062
Application considerations 2063
Working with other FortiOS components 2064
Application traffic shaping 2064
Application control monitor 2065
Enable application control 2065
Application control examples 2068
Intrusion protection 2071
IPS concepts 2071
Enable IPS scanning 2073
IPS processing in an HA cluster 2078
Configure IPS options 2078
Enable IPS packet logging 2081
IPS examples 2082
Custom Application & IPS Signatures 2089
Custom signature syntax 2089
Custom signature keywords 2090
Creating a custom signature to block access to example.com 2101
Creating a custom signature to block the SMTP “vrfy” command 2103
Creating a custom signature to block files according to the file's hash value 2104
Email filter 2106

Email filter concepts 2106
Email filter techniques 2106
Order of spam filtering 2110
Spam actions 2111
Email traffic types to inspect 2111
Configuring an Email Filters 2111
Email filter examples 2113
Data leak prevention 2116
Data leak prevention concepts 2116
DLP archiving 2122
Enable data leak prevention 2123
Creating/editing a DLP sensor 2124
DLP examples 2126
ICAP 2132
The Protocol 2132
Offloading using ICAP 2133
Configuration Settings 2133
Example ICAP sequence 2134
Example Scenario 2134
Other Security Profiles considerations 2137
Security Profiles and Virtual domains (VDOMs) 2137
Conserve mode 2137
SSL content scanning and inspection 2140
Using wildcards and Perl regular expressions 2143
Chapter 22 - SSL VPN 2148
Introduction to SSL VPN 2149
SSL VPN modes of operation 2150
Port forwarding mode 2152
Traveling and security 2153
SSL VPN and IPv6 2154
Basic configuration 2155
User accounts and groups 2155
Configuring SSL VPN web portals 2160
Configuring security policies 2167
Configuring encryption key algorithms 2173
Additional configuration options 2173
The SSL VPN client 2182
FortiClient 2182
Tunnel mode client configuration 2182
The SSL VPN web portal 2184
Connecting to the FortiGate unit 2184
Web portal overview 2184

Portal configuration 2186
Using the My Bookmarks widget 2192
Using the Connection Tool 2194
Tunnel-mode features 2198
Using the SSL VPN virtual desktop 2198
Using FortiClient 2199
Setup examples 2200
Secure Internet browsing 2200
Split Tunnel 2203
Multiple user groups with different access permissions 2205
Troubleshooting 2211
Chapter 23 - System Administration 2214
Using the CLI 2215
Connecting to the CLI 2215
Command syntax 2220
Sub-commands 2225
Permissions 2231
Tips 2231
Firmware 2243
Backing up the current configuration 2243
Restoring a configuration file 2243
Downloading firmware 2244
Testing new firmware 2245
Upgrading the firmware - web-based manager 2246
Upgrading the firmware - CLI 2247
Installing firmware from a system reboot using the CLI 2248
Reverting to a previous firmware version - web-based manager 2249
Reverting to a previous firmware version - CLI 2250
Configuration revision 2251
Controlled upgrade 2251
Interfaces 2253
Physical 2253
Interface settings 2255
Software switch 2261
Virtual Switch 2263
Loopback interfaces 2264
Redundant interfaces 2264
One-armed sniffer 2265
Aggregate Interfaces 2265
DHCP addressing mode on an interface 2267
PPPoE addressing mode on an interface 2268
Administrative access 2271

Wireless 2272
Interface MTU packet size 2272
Secondary IP addresses to an interface 2273
Virtual domains 2273
Virtual LANs 2275
Zones 2276
Probing interfaces 2277
Central management 2278
Adding a FortiGate to FortiManager 2278
Configuration through FortiManager 2280
Firmware updates 2280
FortiGuard 2281
Backup and restore configurations 2281
Administrative domains 2281
Monitoring 2283
Dashboard 2283
sFlow 2284
Monitor menus 2285
Logging 2285
Packet Capture 2289
Alert email 2290
SNMP 2291
SNMP get command syntax 2299
VLANs 2301
VLAN ID rules 2301
VLAN switching and routing 2302
VLANs in NAT mode 2309
Example VLAN configuration in NAT mode 2313
VLANs in transparent mode 2321
Troubleshooting VLAN issues 2330
PPTP and L2TP 2335
How PPTP VPNs work 2335
FortiGate unit as a PPTP server 2337
Configuring the FortiGate unit for PPTP VPN 2340
Configuring the FortiGate unit for PPTP pass through 2340
Testing PPTP VPN connections 2342
Logging VPN events 2342
Configuring L2TP VPNs 2343
L2TP configuration overview 2345
Session helpers 2349
Viewing the session helper configuration 2349
Changing the session helper configuration 2350

DCE-RPC session helper (dcerpc) 2352
DNS session helpers (dns-tcp and dns-udp) 2353
File transfer protocol (FTP) session helper (ftp) 2353
H.245 session helpers (h245I and h245O) 2353
H.323 and RAS session helpers (h323 and ras) 2353
Media Gateway Controller Protocol (MGCP) session helper (mgcp) 2354
ONC-RPC portmapper session helper (pmap) 2354
PPTP session helper for PPTP traffic (pptp) 2355
Remote shell session helper (rsh) 2356
Real-Time Streaming Protocol (RTSP) session helper (rtsp) 2356
Session Initiation Protocol (SIP) session helper (sip) 2357
Trivial File Transfer Protocol (TFTP) session helper (tftp) 2357
Oracle TNS listener session helper (tns) 2357
Advanced concepts 2358
Dual internet connections (redundant Internet connections) 2358
Single firewall vs. multiple virtual domains 2362
Modem 2365
FortiExtender 2368
DHCP servers and relays 2371
Assigning IP address by MAC address 2374
DNS services 2375
Dynamic DNS 2377
FortiClient discovery and registration 2378
IP addresses for self-originated traffic 2379
Administration for schools 2380
Replacement messages list 2383
Disk 2388
CLI Scripts 2388
Rejecting PING requests 2389
Opening TCP 113 2390
Obfuscate HTTP responses 2390
Chapter 24 - Traffic Shaping 2391
The purpose of traffic shaping 2392
Quality of Service 2392
Traffic policing 2393
Bandwidth guarantee, limit, and priority interactions 2394
FortiGate traffic 2394
Through traffic 2395
Important considerations 2398
Traffic shaping methods 2401
Traffic shaping options 2401
Shared policy shaping 2401

Per-IP shaping 2405
Per-IP traffic shaping configuration settings 2406
Adding Per-IP traffic shapers to a security policy 2407
Application control shaping 2407
Enabling traffic shaping in the security policy 2408
Type of Service priority 2410
Differentiated Services 2411
DSCP examples 2412
ToS and DSCP traffic mapping 2415
Traffic Shaper Monitor 2417
Examples 2418
QoS using priority from security policies 2418
QoS using priority from ToS or differentiated services 2420
Example setup for VoIP 2421
Troubleshooting traffic shaping 2425
Interface diagnosis 2425
Shaper diagnose commands 2425
Packet lost with the debug flow 2427
Session list details with dual traffic shaper 2427
Additional Information 2427
Chapter 25 - Transparent Mode 2429
What is Transparent Mode? 2429
Feature matrix - Maximum values 2430
FortiGate features and capabilities matrix - NAT vs Transparent mode 2431
Interfaces in Transparent Mode 2433
Installation 2433
Installing a FortiGate in Transparent mode 2433
Using Port Pairing to Simplify Transparent Mode 2434
Networking 2435
Introduction 2435
Packet Forwarding 2435
NAT 2440
VLANs and Forwarding Domains 2441
Other 2444
Firewall policies 2447
Firewall policy look up 2447
Security scanning 2448
Firewall session list 2448
ISF ACL policies 2448
FortiGate remote management 2449
Management IP configuration in Transparent mode 2449
FortiManager, FortiAnalyzer 2450

Transparent mode and HA 2451
Transparent mode and HA 2451
HA MAC address assignment 2451
Virtual cluster 2451
IPsec VPN in Transparent mode 2452
Rules and details 2452
Example 1 - remote sites in different subnets 2453
Example 2 - remote sites in the same subnet and one remote subnet 2458
Configuration of FortiGate 1 (FGT1): 2459
Configuration of FortiGate 2 (FGT2): 2460
Troubleshooting procedure 2462
Replay traffic scenario 2464
Replay traffic scenario 2464
Transparent mode reminder and best practices 2465
Chapter 26 - Troubleshooting 2467
Troubleshooting methodologies 2468
Establish a baseline 2468
Define the problem 2469
Gathering Facts 2470
Create a troubleshooting plan 2471
Obtain any required additional equipment 2471
Ensure you have administrator level access to required equipment 2472
Contact Fortinet customer support for assistance 2472
Troubleshooting tools 2473
FortiOS diagnostics 2473
FortiOS ports 2501
FortiAnalyzer/FortiManager ports 2502
FortiGuard troubleshooting 2503
Common questions 2506
How to check hardware connections 2507
How to check FortiOS network settings 2508
How to check CPU and memory resources 2509
How to check modem status 2514
How to run ping and traceroute 2514
How to check the logs 2518
How to verify the contents of the routing table (in NAT mode) 2519
How to verify the correct route is being used 2520
How to verify the correct firewall policy is being used 2521
How to check the bridging information in Transparent mode 2521
How to check number of sessions used by UTM proxy 2523
How to examine the firewall session list 2526
How to check wireless information 2527

How to verify FortiGuard connectivity 2528
How to perform a sniffer trace (CLI and Packet Capture) 2528
How to debug the packet flow 2531
Troubleshooting resources 2532
Technical Documentation 2532
Fortinet Video Library 2532
Release Notes 2532
Knowledge Base 2532
Fortinet Technical Discussion Forums 2532
Fortinet Training Services Online Campus 2532
Fortinet Customer Support 2533
Technical Support Organization Overview 2534
Fortinet Global Customer Services Organization 2534
Creating an account 2535
Registering a device 2536
Reporting problems 2538
Assisting technical support 2539
Support priority levels 2539
Return material authorization process 2540
Chapter 27 - Virtual Domains 2542
Virtual Domains 2543
Benefits of Virtual Domains 2543
Enabling and accessing Virtual Domains 2545
Configuring Virtual Domains 2569
Virtual Domains in NAT/Route mode 2577
Virtual domains in NAT/Route mode 2577
Example NAT/Route VDOM configuration 2585
Virtual Domains in Transparent mode 2596
Transparent operation mode 2596
Operation mode differences in VDOMs 2598
Configuring VDOMs in Transparent mode 2599
Example of VDOMs in Transparent mode 2600
Inter-VDOM routing 2615
Benefits of inter-VDOM routing 2615
Getting started with VDOM links 2616
Inter-VDOM configurations 2621
Dynamic routing over inter-VDOM links 2625
HA virtual clusters and VDOM links 2626
Example of inter-VDOM routing 2627
Troubleshooting Virtual Domains 2652
VDOM admin having problems gaining access 2652
FortiGate unit running very slowly 2652

General VDOM tips and troubleshooting 2653
Chapter 28 - VM Installation 2657
FortiGate VM Overview 2658
FortiGate VM models and licensing 2658
Registering FortiGate VM with Customer Service & Support 2659
Downloading the FortiGate VM deployment package 2659
Deployment package contents 2661
Deploying the FortiGate VM appliance 2662
Deployment example – VMware 2663
Open the FortiGate VM OVF file with the vSphere client 2663
Configure FortiGate VM hardware settings 2669
Transparent mode VMware configuration 2670
High Availability VMware configuration 2671
Power on your FortiGate VM 2671
Deployment example – MS Hyper-V 2672
Create the FortiGate VM virtual machine 2672
Configure FortiGate VM hardware settings 2679
High Availability Hyper-V configuration 2690
Start the FortiGate VM 2691
Deployment example – KVM 2692
Create the FortiGate VM virtual machine 2692
Configure FortiGate VM hardware settings 2694
Start the FortiGate VM 2695
Deployment example – OpenXen 2696
Create the FortiGate VM virtual machine (VMM) 2696
Deployment example – Citrix XenServer 2702
Create the FortiGate VM virtual machine (XenCenter) 2702
Configure virtual hardware 2706
FortiGate VM Initial Configuration 2709
Set FortiGate VM port1 IP address 2709
Connect to the FortiGate VM Web-based Manager 2712
Upload the FortiGate VM license file 2712
Validate the FortiGate VM license with FortiManager 2713
Configure your FortiGate VM 2714
Chapter 29 - VoIP Solutions: SIP 2715
FortiGate VoIP solutions–SIP 2716
Common SIP VoIP configurations 2717
SIP messages and media protocols 2723
The SIP session helper 2738
The SIP ALG 2744
SIP ALG configuration overview 2746
Conflicts between the SIP ALG and the session helper 2749

Stateful SIP tracking, call termination, and session inactivity timeout 2749
SIP and RTP/RTCP 2751
How the SIP ALG creates RTP pinholes 2751
Configuration example: SIP in Transparent Mode 2754
RTP enable/disable (RTP bypass) 2757
Opening and closing SIP register, contact, via and record-route pinholes 2757
Accepting SIP register responses 2758
How the SIP ALG performs NAT 2758
Enhancing SIP pinhole security 2783
Hosted NAT traversal 2786
SIP over IPv6 2791
Deep SIP message inspection 2792
Blocking SIP request messages 2797
SIP rate limiting 2799
SIP logging and DLP archiving 2801
Inspecting SIP over SSL/TLS (secure SIP) 2801
SIP and HA–session failover and geographic redundancy 2804
SIP and IPS 2807
SIP debugging 2807
Chapter 30 - WAN Optimization, Web Cache, Explicit Proxy, and WCCP 2812
Example network topologies 2813
Basic WAN optimization topology 2813
Out-of-path WAN Optimization topology 2814
Topology for multiple networks 2816
WAN optimization with web caching 2817
WAN optimization and web caching with FortiClient peers 2818
Explicit Web proxy topologies 2819
Explicit FTP proxy topologies 2821
Web caching topologies 2822
WCCP topologies 2824
Configuring WAN optimization 2826
Client/server architecture 2826
WAN optimization peers 2828
Manual (peer-to-peer) and active-passive WAN optimization 2828
WAN optimization profiles 2831
Protocol optimization 2833
Protocol optimization and MAPI 2834
Byte caching 2834
WAN optimization transparent mode 2835
FortiClient WAN optimization 2836
Operating modes and VDOMs 2836
WAN optimization tunnels 2836

WAN optimization and user and device identity policies, load balancing and traffic shaping 2838
WAN optimization and HA 2839
WAN optimization, web caching and memory usage 2839
Monitoring WAN optimization performance 2839
WAN optimization configuration summary 2841
Best practices 2844
Peers and authentication groups 2845
Basic WAN optimization peer requirements 2845
How FortiGate units process tunnel requests for peer authentication 2845
Configuring peers 2846
Configuring authentication groups 2847
Secure tunneling 2849
Monitoring WAN optimization peer performance 2850
Configuration examples 2851
Example Basic manual (peer-to-peer) WAN optimization configuration 2851
Example Active-passive WAN optimization 2858
Example Adding secure tunneling to an active-passive WAN optimization configuration 2866
Web caching and SSL offloading 2875
Turning on web caching for HTTP and HTTPS traffic 2875
Turning on web caching for HTTPS traffic 2876
Changing the ports on which to look for HTTP and HTTPS traffic to cache 2879
Web caching and HA 2880
Web caching and memory usage 2880
Changing web cache settings 2880
Forwarding URLs to forwarding servers and exempting web sites from web caching 2883
Monitoring Web caching performance 2884
Example Web caching of HTTP and HTTPS Internet content for users on an internal network 2885
Example reverse proxy web caching and SSL offloading for an Internet web server using a static one-to-one virtual IP 2888
Network topology and assumptions 2888
FortiClient WAN optimization 2893
FortiClient WAN optimization over IPsec VPN configuration example 2893
The FortiGate explicit web proxy 2897
General explicit web proxy configuration steps 2899
Proxy auto-config (PAC) configuration 2903
Unknown HTTP version 2903
Authentication realm 2903
Other explicit web proxy options 2904
Configuring an external IP address for the IPv4 explicit web proxy 2904
Configuring an external IP address for the IPv6 explicit web proxy 2904

Restricting the IP address of the IPv4 explicit web proxy 2904
Restricting the outgoing source IP address of the IPv4 explicit web proxy 2905
Restricting the IP address of the explicit IPv6 web proxy 2905
Restricting the outgoing source IP address of the IPv6 explicit web proxy 2905
Proxy chaining (web proxy forwarding servers) 2905
Explicit web proxy authentication 2909
Security profiles, threat weight, device identification, and the explicit web proxy 2912
Web Proxy firewall services and service groups 2912
Explicit web proxy firewall address URL patterns 2913
Changing HTTP headers 2914
Preventing the explicit web proxy from changing source addresses 2914
Explicit web proxy sessions and user limits 2920
The FortiGate explicit FTP proxy 2922
How to use the explicit FTP proxy to connect to an FTP server 2924
General explicit FTP proxy configuration steps 2926
Restricting the IP address of the explicit FTP proxy 2928
Restricting the outgoing source IP address of the explicit FTP proxy 2928
Security profiles, threat weight, device identification, and the explicit FTP proxy 2929
Example users on an internal network connecting to FTP servers on the Internet through the explicit FTP with RADIUS authentication and virus scanning 2929
Explicit FTP proxy sessions and user limits 2934
FortiGate WCCP 2935
WCCP service groups, service numbers, service IDs and well known services 2935
WCCP configuration overview 2939
Example caching HTTP sessions on port 80 using WCCP 2939
Example caching HTTP sessions on port 80 and HTTPS sessions on port 443 using WCCP 2942
WCCP packet flow 2944
Configuring the forward and return methods and adding authentication 2944
WCCP Messages 2945
Troubleshooting WCCP 2945
Diagnose commands 2947
get test {wad | wccpd} <test_level> 2947
diagnose wad 2948
diagnose wacs 2951
diagnose wadbd 2952
diagnose debug application {wad | wccpd} [<debug_level>] 2952
diagnose test application wad 2200 2952
Appendix A - Open Ports Diagrams 2955
Open Ports Diagrams 2955
Appendix B - FortiGate Modem Compatibility Matrix 2956
FortiGate Modem Compatibility Matrix 2956

To find the modem list (FortiOS 5.2) - web-based manager: 2956
Appendix C - FortiExtender Modem Compatibility Matrix 2962
FortiExtender Modem Compatibility Matrix 2962
To find the FortiExtender Modem list (FortiOS 5.2) - web-based manager: 2962

Chapter 1 - What's New for FortiOS 5.2

This FortiOS Handbook chapter contains the following sections:

- New features in FortiOS 5.2.12 provides a brief description of features that were added to FortiOS 5.2.12.
- New features in FortiOS 5.2.9 provides a brief description of features that were added to FortiOS 5.2.9.
- New features in FortiOS 5.2.8 provides a brief description of features that were added to FortiOS 5.2.8.
- New features in FortiOS 5.2.5 provides a brief description of features that were added to FortiOS 5.2.5.
- New features in FortiOS 5.2.4 provides a brief description of features that were added to FortiOS 5.2.4.
- New features in FortiOS 5.2.3 provides a brief description of features that were added to FortiOS 5.2.3.
- New features in FortiOS 5.2.2 provides a brief description of features that were added to FortiOS 5.2.2.
- New features in FortiOS 5.2.1 provides a brief description of features that were added to FortiOS 5.2.1.
- Top Features described some of the most important new features in FortiOS 5.2.
- System Features contains information on features connected to global settings.
- Usability Enhancements describes some enhancements that make the web-based manager easier to use and more effective.
- The next sections deal with new features for specific areas of network configuration:
  - Firewall
  - Security Profiles
  - IPsec VPN
  - SSL VPN
  - Authentication
  - Managing Devices
  - Wireless Networking
  - IPv6
  - High Availability
  - WAN Optimization, Web Cache, and Explicit Proxy
  - Advanced Routing
  - Logging and Reporting
- Other New Features contains information about other features that have been added in FortiOS 5.2.
- RFC List contains information about RFCs that are supported by the new features.

New features in FortiOS 5.2.12

Most development work in FortiOS 5.2.12 involved resolving issues. However, there were a few new features as well.

Stackable VDOM licenses (269153)

VDOM licenses are now stackable, allowing you to buy additional licenses and stack them on top existing licenses to increase the number of VDOMs you can have.

New features in FortiOS 5.2.9

Most development work in FortiOS 5.2.9 involved resolving issues. However, there were a few new features as well.

Last session information saved in a crash log when an IPS engine crash occurs (378252)

Changes to FortiOS IPS and to the IPS engine version 3.170 now cause FortiOS to save a crash log with the last session information when an IPS crash occurs. This information can be used by Fortinet support to diagnose the cause of the crash.

Dynamic Frequency Selection (DFS) support added to the FortiAP-321C (369052)

FortiOS 5.2.9 now supports DFS for the FortiAP-321C.

New features in FortiOS 5.2.8

TLS 1.2 support for SSL offloading (241817)

You can use the following command to configure SSL offloading to support TLS 1.2:

```
config firewall vip
   edit <name>
      set type server-load-balance
      set server-type https
      set ssl-min-version tls-1.2
      set ssl-max-version tls-1.2
      ...
```

The default `ssl-min-version` is still `ssl-3.0` and the default `ssl-max-version` is still `tls-1.0` so you have to specifically set at least `ssl-max-version` to `tls-1.2` to enable TLS 1.2 support.

The following AES-GCM TLS 1.2-only cipher suites have also been added. These cipher suites are not supported by the CPx or NPx processors so if you select one of these, all processing is done without hardware acceleration.

TLS 1.2 support does not require setting `ssl-algorithm` to `custom` and configuring a custom cipher suite.

```
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
TLS-RSA-WITH-AES-128-GCM-SHA256
TLS-RSA-WITH-AES-256-GCM-SHA384
```

You can use the following command to select one of these cipher suites:

```
config firewall vip
   edit <name>
      set type server-load-balance
      set server-type https
      set ssl-max-version tls-1.2
      set ssl-algorithm custom
         config ssl-cipher-suites
            edit 100
               set cipher TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
               ...
```

New features in FortiOS 5.2.5

The default Diffie-Hellman setting is 2048 (286801)

This change improves the security of Diffie-Hellman key generation. The default was 1024.

Simple, Wildcard & Regex options now available for per-user BWL (270165)

The **Allow users to override blocked categories** web filter profile feature (available on some FortiGate models) now allows users to use simple, wildcard and regex expressions to identify the URLs that are blocked.

This feature is also called per-user BWL. To be able to configure this feature from the GUI enter the following command:

```
config system global
   set per-user-bwl enable
end
```

Then go to **Security Profiles > Web Filtering**, edit a web filtering profile and select **Allow users to override blocked categories**. You can select a web filter profile that users can switch to. If the URLs in the web filter profile contain wildcards or regex expressions they will now work when selected for user overrides.

Use the following command to configure this feature from the CLI:

```
config webfilter profile
   edit <profile-name>
      set options per-user-bwl
         config override
            set profile
            ...
         end
   end
```

New diagnose traffictest command (280801)

```
diagnose traffictest {show | run -h arg | server-intf | client-intf | port | proto}
```

Where -h arg can be

-f, --format [kmgKMG] format to report: Kbits, Mbits, KBytes, MBytes

-i, --interval # seconds between periodic bandwidth reports

-F, --file name xmit/recv the specified file

-A, --affinity n/n,m set CPU affinity

-V, --verbose more detailed output

-J, --json output in JSON format

-d, --debug emit debugging output

-v, --version show version information and quit

-h, --help show this message and quit

-b, --bandwidth #[KMG][/#] target bandwidth in bits/sec (0 for unlimited) (default %d Mbit/sec for UDP, unlimited for TCP) (optional slash and packet count for burst mode)

-t, --time # time in seconds to transmit for (default %d secs)

-n, --bytes #[KMG] number of bytes to transmit (instead of -t)

-k, --blockcount #[KMG] number of blocks (packets) to transmit (instead of -t or -n)

-l, --len #[KMG] length of buffer to read or write (default %d KB for TCP, %d KB for UDP)

-P, --parallel # number of parallel client streams to run

-R, --reverse run in reverse mode (server sends, client receives)

-w, --window #[KMG] TCP window size (socket buffer size)

-C, --linux-congestion <algo> set TCP congestion control algorithm (Linux only)

-M, --set-mss # set TCP maximum segment size (MTU - 40 bytes)

-N, --nodelay set TCP no delay, disabling Nagle's Algorithm

-4, --version4 only use IPv4

-6, --version6 only use IPv6

-S, --tos N set the IP 'type of service'

-L, --flowlabel N set the IPv6 flow label (only supported on Linux)

-Z, --zerocopy use a 'zero copy' method of sending data

-O, --omit N omit the first n seconds

-T, --title str prefix every output line with this string

--get-server-output get results from server

[KMG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

Improve device identification (289921)

FortiFone devices are now identified by FortiOS as **Fortinet FON**. As Apple device detection have also been improved. FortiOS can now more reliably detect Mac OS, iPhone 6, Apple Watch, Microsoft tables and so on.

NP6 SynProxy Monitoring (218425)

New support for monitoring SynProxy and other DoS anomalies. The DoS policy list for both IPv4 and IPv6 displays active IPS meters, as shown by IP and by anomaly. With SynProxy activated, each destination IP will show results.

Maximum number of VLANs per interface increased for the FortiGate-30 Series (300032)

On the FortiGate-30 series products you can add up to 20 VLANs to a physical interface.

New features in FortiOS 5.2.4

This chapter lists new features added to FortiOS 5.2.4:

- The FortiGate-1000D now supports WAN Optimization. (275801)
- Split FortiGate-3810D 100G ports into ten 10G ports. For more information, see Split 40G ports on some FortiGate models on page 53(263829)

  Enter the following command to enable split ports for port1 and port2:

  ```
  config system global
     set split-port port23 port26
  end
  ```

  When you enter this command the FortiGate reboots and when it starts up the ports are split. The GUI and CLI would show these split ports as port1/1, port1/2, port1/3, ... port2/4.
- The `diagnose hardware device disk` command now includes the the `MAX SSD Disk` field, which shows the number of functioning SSD disks installed in the FortiGate. (271115)
- The correct checksum and file-size information, provided by the AV engine, is now added to anti-virus log messages. (261885)
- FGCP high availability supports BFD enabled BGP graceful restart after an HA failover. (255574)
- You can add a TFTP server address and a file name to a DHCP server configuration on one FortiGate to contain information that can be used by other FortiGates to download firmware updates from that TFTP server. This feature was added in a previous release but has been improved for FortiOS 5.2.4. (270160)

  Use the following command to add a TFTP server IP address of 10.10.10.5 and firmware image filename image.out to a FortiGate DHCP server:

  ```
  config system dhcp server
     edit 0
        ...
        set tftp-server 10.10.10.5
        set filename image.out
        ...
     end
  ```

  Then on a second FortiGate you can use the following command to cause the second FortiGate to retrieve the TFTP server IP address and firmware image filename and then download the firmware image and updgrade its firmware. In this example, the wan1 interface of the second FortiGate must be able to connect to the DHCP server of the original FortiGate.

  ```
  execute restore config dhcp wan1
  ```
- The default FortiGuard IPS and AV database update interval is now every 2 hours. Previously it was daily. (278772)

The new default configuration is:

```
config system autoupdate schedule
   set status enable
   set frequency every
   set time 2:60
end
```

where when `frequency` is set to `every` and `time` is `hh:mm`. If `mm` is 60 the update occurs at a random time within the final hour of the frequency. So a `time` of 2:60 means the update will occur some time in the second hour.

- WiFi logging improvements. (211695)

  Improved FortiWiFi local radio tx/rx statistics support.

  Band and channel_bonding fields added to oper-channel wireless event log.

  AP field is now accurately added to event log messages when radio settings are changed.

  Radio number(radioid) field added to wireless client activity event log.

- The extended IPS database is enabled by default for models with multiple CP8 content processors (300D/500D/1000D/1200D/1500D/3700D/3700DX/3810D/5001D). (238338)
- A new **block-security-risks** default webfilter profile has been added. In this profile FortiGuard Categories is selected,the Security Risk category is blocked, the Unrated catagory is set to warning and Rate URLs by Domain and IP Address is enabled. (278767)
- Changes to disk logging and WAN Optimization depending on the FortiGate hard disk configuration (adjustments/refinements to the changes made in 5.2.3). (266032)

  When you upgrade your FortiGate unit to FortiOS 5.2.4:

  - If your FortiGate unit has one hard disk, WAN Optimization settings will only be available from the CLI.
  - If your FortiGate unit has two hard disks, WAN Optimization settings will be available from the GUI and CLI.
  - WAN Optimization is not available if your FortiGate unit does not have a hard disk.

  The FortiOS 5.2.4 Feature/Platform Matrix shows WAN Optimization support by FortiGate model.

- For multi-hop EBGP peers, the nexthop is modified by the `route-map-out` setting. (183637)
- On FortiGate models that support it, the Fortinet_Factory certificate is now 2048 bits and uses SHA2. (284419)
- Explicit web proxy authentication performance improvements to prevent authenticated users from being blocked. (276065)
- Geography firewall addresses can now be added to explicit web proxy policies from the GUI and CLI. (281461)
- Add options for strict OCSP and strict CRL certificate checking (0258979)
  The new command options are:

  ```
  config vpn certificate setting
     set strict-crl-check {disable | enable}
     set strict-ocsp-check {disable | enable}
  end
  ```

  Enable `strict-crl-check` to enable strict mode CRL checking. If strict checking is not enabled and a certificate is found to be on a CRL list, the certificate can be used and a warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being recorded.

  Enable `strict-ocsp-check` to enable strict mode OCSP checking. If strict checking is not enabled and an OCSP server responds with “cert status unknown” the certificate can be used and a

warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being written.

New features in FortiOS 5.2.3

This chapter provides a brief introduction to the following features that were added to FortiOS 5.2.3. See the release notes for a complete list of new features/resolved issues in this release.

- Interfaces on some FortiGate models are set in one-arm sniffer mode by default
- Merge FGT-20C-ADSL and FWF-20C-ADSL
- Log Viewer Improvements
- Add AeroScout Inter-operabiliy testing
- Add "Last connection time" Column in FortiView > VPN
- FSSO agent support OU in group filters
- Certificate GUI improvements
- Improvement to WAN optimization feature
- Add FortiAP LED dark support
- Allow user to change VDOM operation mode more easily
- Support 4x10G interfaces in 5001D 40G ports
- Allow admin user to start/defer file system check if FGT was not shutdown properly
- Cloud Sandboxing
- Add a tooltip to remind users to activate FortiCloud to enable FortiSandbox cloud
- Add warn about factory default certificate
- Deep Flow

Interfaces on some FortiGate models are set in one-arm sniffer mode by default

Fort example:

- By default the FortiGate-300D port4 and port8 interfaces are in sniffer mode.
- By default the FortiGate-500D port5, port6, port13, and port14 interfaces are in sniffer mode.
- Other models may have similar default settings.

If you want to use these interfaces for other purposes you can change their mode from the GUI or CLI. From the GUI just go to **System > Network > Interface**, edit the interface and change its addressing mode as required.

Merge FGT-20C-ADSL and FWF-20C-ADSL

Add `set wan enable` to set one of the switch port as WAN port. By default, there is no WAN port for FWF-20C-ADSL and FGT-20C-ADSL.

CLI changes

Add `set wan enable` command.

Syntax

```
config system global
   set wan [enable|disable] //disable by default
end
```

This CLI command enables one of the switch port (LAN4 for 20C-ADSL) as wan port. In this way, a redundant WAN port is supported besides ADSL port.

By setting LAN4 into a switch port (set wan disable) or a dedicated WAN port (set wan enable), the two platforms can work in two modes:

1. ADSL + LAN (LAN1,LAN2,LAN3,LAN4 as one switch)
2. ADSL + LAN (LAN1,LAN2,LAN3 as one switch) plus WAN interface. Please note that:

- The option to switch between the two modes can be CLI-only.
- When switching between the 2 modes, a reboot is expected.
- `Set wan disable` won't take effect if WAN interface is in use.

Log Viewer Improvements

Extends Faceted Search portion of FortiView to support complicated sorting.

Improves usability of log viewer bottom pane with flexbox and css animations.

Allows filtering of combined column's constituent parts.

GUI changes

Replaced column filter icon on header with faceted search bar. Bottom panel now behaves better and resizes smoothly.

Add AeroScout Inter-operabiliy testing

Syntax

```
config wireless-controller wtp-profile
   edit <wtp-profile>
      config lbs
         set aeroscount Enable/disable
         set aeroscout-server-ip xxx.xxx.xxx.xxx // IP address of AeroScout server.
         set aeroscout-server-port <integer> // AeroScout server UDP listening port (1024 65535)
         set aeroscout-mu-factor <integer> // AeroScout dilution factor for Mobile Unit (MU) mode (default
             = 20)
         set aeroscout-mu-timeout <integer> // AeroScout dilution timeout (sec) for Mobile Unit (MU) mode
             (default = 5s)
      end
   next
end
```

Add "Last connection time" Column in FortiView > VPN

Users can sort by number of connections, duration and total bytes but cannot see the last time the user connected.

GUI changes

A ***Last connection time*** column has been added which can simply indicate the timestamps of the last VPN connection that was started for that user.

The user should be able to sort by ***last connection time***.

FSSO agent support OU in group filters

Previously, in FSSO configuration GUI page, via LDAP browser, admin can select user/group filters to send to FSSO Agent. Now that FSSO Agent supports OU filter. So GUI is updated to allow admin to select OU from LDAP browser.

GUI Changes

When creating FSSO group from Users/Groups creation wizard, in the LDAP browser, there is a new tab named ***Organizational Unit*** next to Users and Groups tab. This new tab can also be seen in FSSO dialog.

Certificate GUI improvements

Some GUI changes include:

- The table, under ***System > Certificates*** fit in one regular browser width by default, similar to ***Policy***, ***Interface*** and other pages.
- Wrap the text in the cells to keep the columns narrower.
- Improve the columns displayed to include:
  - Who signed it (where applicable).
  - Expiry date.
- Do not list certificates that do not exist on the FortiGate.

Improvement to WAN optimization feature

In some models WAN Optimization configuration can now be done from the CLI, you can still do GUI configuration after enabling GUI configuration from the CLI using following command:

```
config system global
   set gui-wanopt-cache enable
end
```

For more information, refer to the 5.2.3 feature/platform matrix at the following link:

http://docs.fortinet.com/d/fortigate-fortios-5.2.3-feature-platform-matrix

Add FortiAP LED dark support

Few customers want to keep their APs as discrete as possible, and want an option to run dark by turning off all LEDs.

Syntax

```
config wireless-controller wtp-profile
   edit "profile"
      set led-state enable|disable
   end
```

```
end
```

By default, led-state is set to enable.

FortiAP side:

```
cfg -a LED_STATE=0|1|2
```

0:LED is on, 1:LED is off, 2: LED is controlled by the controller (FortiGate).

By default, `LED_STATE` is set to 2. If it is set to 2, FortiAP will take `led-state` setting configured on the controller. If it is set to 0 or 1, FortiAP will ignore `led-state` setting configured on the controller.

Allow user to change VDOM operation mode more easily

Allow user to switch between NAT and TP mode without having to manually remove a large selection of configuration, this can be achieved using CLI and GUI.

Split 40G ports on some FortiGate models

On FortiGate models with 40G interfaces, such as the FortiGate-5001D and 3700D you can now split a single 40G interface into four 10G interfaces. Enabling split ports adjusts NP6 mapping.

Enter the following command to enable split ports for port1 and port2:

```
config system global
   set split-port port1 port2
end
```

When you enter this command the FortiGate reboots and when it starts up the ports are split. The GUI and CLI would show these split ports as port1/1, port1/2, port1/3, ... port2/4.

Allow admin user to start/defer file system check if FGT was not shutdown properly

When FGT wasn't shutdown properly, we don't start the file system check yet as it may takes time. Instead, after admin user logins, a dialog is shown offering admin user to start file system check or defer later. If file system check is chosen, FGT will be rebooted and file system check is started.

Cloud Sandboxing

FortiStandbox Settings is accessible under ***System > Config > FortiSandbox***, a new ***FortiSandbox Cloud*** option is available. When selected, it uses ***FortiCloud Account*** configured previously in the ***License Information*** widget.

Add a tooltip to remind users to activate FortiCloud to enable FortiSandbox cloud

FortiSandbox Cloud option is grayed out on the FortiSandbox settings page if FortiCloud account is not activated. Added a tooltip to remind users to activate FortiCloud to enable FortiSandbox cloud, also added a tool help element beside the FortiSandbox input that contains a helpful tips on how to enable FortiSandbox.

Add warn about factory default certificate

Default SSL-VPN server certificate has been changed from self-signed certificate to Fortinet_Factory certificate. When SSL-VPN is configured with a default certificate, show a warning on both the SSL-VPN settings dialog and

the policy dialog, recommending the use a proper signed certificate for better security.

Deep Flow

This new inspection mode uses IPS scan similar to Flow mode to catch anything obvious covered by signatures, but passing a copy of anything over 64 bytes to the scanunit engine to collect the parts of the payload for proxy style analysis, while the chunks of payload are sent to the recipient just as if it were in flow mode.

Once the last chunk of the payload is received by the scanunit engine, it is analyzed. If it successfully passes analysis the last chunk is sent off to the recipient.

This method is characterized as being as secure and effective as proxy mode but faster then regular Flow mode.

When configuring Deep Flow, GUI and CLI shows this option as Flow but the functionality as described earlier.

New features in FortiOS 5.2.2

This chapter provides a brief introduction to the following features that were added to FortiOS 5.2.2. See the release notes for a complete list of new features/resolved issues in this release.

- Add allocator API and counters to scanunit
- Add tooltips for application categories
- Add broadcast/multicast suppression for local bridge mode ssid on the FAP side
- Add hardware switch feature and SPAN functionality to 30D, 60, and 90D. Move POE ports out of Internal switch to independent interfaces
- Disable performance statistics Logging
- Improvements to firmware upload GUI dialog
- Reimplementation of the session list as a part of FortiView to improve functionality and usability
- Add GUI option to control the TLS versions for web administration
- Cloud Wifi Support
- Merge FWF/FGT-60D-3G4G and FGR-60D
- Add FAP-224D/222C/25D/214B/21D/24D/112D/223C/321C support
- Add support for more than 32k FortiClient configuration distribution through EC-NAC
- Add a warning when using deep SSL inspection mode on security policy and SSL profile pages
- Improve FSSO group GUI
- Add Log Rate stats to System Resources widget
- Add a command to export logs on local disk to external USB
- Improve FortiView performance and add System Events, Admin Logins, and VPN
- Integrate vmtools for FortiGate VMWare platforms

Add allocator API and counters to scanunit

Add a new memory management wrapper and statistics framework for scanunit to improve memory accounting.

CLI changes

Add diagnose sys scanunit stats command.

Syntax

```
diagnose sys scanunit stats <option>
```

Option	Description
list	List all statistics.
all	List all statistics.
clear	Clear all statistics.

Add diagnose sys scanunit filter command.

Syntax

```
diagnose sys scanunit filter <option>
```

Option	Description
list	Display the current filter.
clear	Clear the current filter.
negate	Negate the specified filter parameter.
vd	Index of virtual domain. -1 matches all.
worker	Index of worker. -1 matches all.

Add diagnose sys scanunit log filter command.

Syntax

```
diagnose sys scanunit log filter <option>
```

Option	Description
list	Display the current scanunit log filter.
clear	Clear the current scanunit log filter.
negate	Negate the specified filter parameter.
vd	Index of virtual domain. -1 matches all.
worker	Index of worker. -1 matches all.

Add diagnose sys scanunit restart command.

Syntax

```
diagnose sys scanunit restart
```

Add tooltips for application categories

Implementation of a tool tip for application category which are available in ***FortiView > applications*** ,and under ***Log & Report > traffic log***. For known categories, it provides a short description for the application category - this comes from FortiGuard app categories description. For unknown categories, the traffic has been scanned but the traffic pattern does not match any signature.

Add broadcast/multicast suppression for local bridge mode ssid on the FAP side

CLI changes

Add broadcast/multicast suppression for different packet type.

Syntax

```
conf wireless-controller vap
   edit <vap_name>
   set broadcast-suppression <option>
end
```

Option	Description
dhcp-up	Suppress broadcast uplink DHCP messages.
dhcp-down	Suppress broadcast downlink DHCP messages.
arp-known	Suppress broadcast ARP for known wireless clients.
arp-unknown	Suppress broadcast ARP for unknown wireless clients.
arp-reply	Suppress broadcast ARP reply from wireless clients.
netbios-ns	Suppress NetBIOS name services packets with UDP port 137.
netbios-ds	Suppress NetBIOS datagram services packets with UDP port 138.
ipv6	Suppress IPv6 packets.

Add hardware switch feature and SPAN functionality to 30D, 60, and 90D. Move POE ports out of Internal switch to independent interfaces.

Added virtual switch commands.

Syntax

```
config system virtual-switch
   edit lan
      set physical-switch sw0
         config port
            edit port1
            next
            edit port2
            next
         end
   next
end
```

Disable performance statistics Logging

A new CLI option `sys-perf-log-interval` was added into `config system global` section

Syntax

```
config system global
   set sys-perf-log-interval <value>
end
```

`value` is performance statistics logging interval (1 - 15 min, 0 = disable).

The default value of `sys-perf-log-interval` attribute is 5 minutes.

This attribute only affects the log to FortiAnalyser and/or Syslog, no `perf-stats` log goes to disk or FortiCloud no matter what the value is.

Improvements to firmware upload GUI dialog

A few items to consider for firmware upgrades:

- Maintain the upgrade path on FortiGuard with recommended version information.
- Allow user to easily upgrade to the recommended version.
- Show progress of downloading the image and upgrading, shows progress bar.

GUI changes

On the status page if a new update is available on the FortiGuard server then the next recommended update is displayed.

The admin can click the upgrade link and optionally backup the config before confirming the upgrade.

The dialog can display the progress of the update. Once the update is being installed the browser should probe the FortiGate until it has completed the reboot, then automatically refresh the browser to go to the login screen.

Similarly when going to the upgrade page if the user chooses to upgrade from the FortiGuard Network then the recommended firmware is set in the firmware version box (if any). If no firmware is recommended then "up to date" can be displayed. Note that there may be several firmware options available but he chooser should be set to the recommended version automatically, not just the latest version available. This information should be obtained from the upgrade path package from FortiGuard.

Once the update is complete and reboot starts the browser should try to probe the FortiGate until to responds then redirect to the login page once it is available again.

Reimplementation of the session list as a part of FortiView to improve functionality and usability

New options has been added to enable/disable inclusion of unscanned traffic in FortiView application charts and to enable/disable inclusion of local traffic in FortiView real-time charts.

Remove top sessions dashboard widget.

Syntax

```
config log gui-display
   set fortiview-unscanned-apps enable/disable // inclusion of unscanned traffic in FortiView application
       charts.
   fortiview-local-traffic enable/disable // inclusion of local-in traffic in FortiView realtime charts.
end
```

Add GUI option to control the TLS versions for web administration

Introduce GUI settings to allow admin control the TLS v1.x versions for GUI HTTPS..

Syntax

```
config system global
   set gui-https-tls-version <option>
end
```

Option	Description
tlsv1-0	TLS 1.0.
tlsv1-1	TLS 1.1.
tlsv1-2	TLS 1.2.

Cloud Wifi Support

FortiCloud customer account ID can be specified.

Syntax

```
config wireless-controller setting
   set account-id <string>
end
```

Merge FWF/FGT-60D-3G4G and FGR-60D

Moved `lte modem` command from `system global` to `system lte-modem`, and added `APN, authentication, redundant, extra-init, network type` commands.

CLI changes

Syntax

```
config system lte-modem
   set status enable/disable
   set extra-init STRING
   set authtype none/pap/chap
   set APN STRING
   set mode standalone/redundant
   set net-type CDMA-1x/EV-DO/LTE/Auto //Only available for F*60DC, since the feature only works for Novatel e362 module right now.
   set holddown-timer sec
end
```

Added `diagnose sys lte-modem` command

Syntax

```
diagnose sys lte-modem info
```

Sample output

```
LTE Modem configuration enabled!
LTE Modem device initialized.
Manufacturer: Novatel Wireless Incorporated
Model: E362 WWAN
MEID: 99000094761891
USB Modem Interface: up
SIM State: Valid
ICCID: 89148000000229083036
Signal Strength: 3
Network Type: LTE
Network Cfg: Automatic
APN: vzwinternet
Authen Type: none
Extra Init String:
Interface mode: standalone
Holddown Time: 30
```

GUI changes

GUI is almost the same, the difference is, when LTE Modem is plugged in but not connected, the same info items(vendor/model/iccid/meid etc) are still displayed, this gives more information to users.

Add FAP-224D/222C/25D/214B/21D/24D/112D/223C/321C support

CLI changes

Syntax

```
config wireless-controller wtp-profile
   edit <profile_name>
      config platform
      set type
```

```
        .....
        25D FAP25D
        222C FAP222C
        224D FAP224D
        214B FK214B
        21D FAP21D
        24D FAP24D
        112D FAP112D
        223C FAP223C
        321C FAP321C
    end
end
```

GUI changes

New platform FAP-224D/222C/25D/214B/21D/24D/112D/223C/321C can be selected in wtp profiles.

Add support for more than 32k FortiClient configuration distribution through EC-NAC

A new child table has been added to store advanced configuration greater than 32k

Syntax

```
config endpoint-control profile
   edit <profile_name>
      config forticlient-winmac-settings
         config extra-buffer-entries
            edit entry_id
            set buffer <string>
            next
         end
      end
   next
end
```

Add a warning when using deep SSL inspection mode on security policy and SSL profile pages

A help text has been added when enabling SSL deep inspection.

GUI changes

Add an information bubble on the firewall policy page, as well as in the SSL profile page when enabling or selecting deep inspection.

Add a video link via videos menu to both of the above pages to link to a new video that instructs users how to install these certificates throughout the network.

Improve FSSO group GUI

Apply new LDAP Browser to FSSO GUI pages allowing creating and updating FSSO group from the firewall policy page.

GUI changes

In the firewall policy edit dialog, clicking on the ***Create Users/Groups*** button on the bottom of the ***Source User (s***) drop-down list will launch the Wizard.

This is an extended version of the ***Users/Groups Creation Wizard*** which has extra option to create FSSO group. Clicking on ***FSSO*** will show the process of creating and/or updating FSSO group.

This new LDAP browser design has been applied to the ***Single Sign-On*** edit page.

Add Log Rate stats to System Resources widget

Log rate of disk and FortiAnalyser are shown in the ***System Resources*** widget when they were enabled.

Add a command to export logs on local disk to external USB

CLI changes

Add a command to backup all log files to USB drive.

Syntax

```
execute backup disk alllogs usb
```

Add a command to backup specific log file(s) to USB drive.

Syntax

```
execute backup disk log usb <string> //Choose log: traffic, event, ips, virus, webfilter, spam, dlp, voip, app-ctrl, anomaly, netscan
```

Improve FortiView performance and add System Events, Admin Logins, and VPN

GUI changes

Three new menu items has been added under ***FortiView***

- ***System Events***
- ***Admin Logins***
- ***VPN***

Integrate vmtools for FortiGate VMWare platforms

Open-vm-tools project is used as basis for new daemon.

CLI changes

Add a command to debug vmtools.

Syntax

```
diagnose debug application vmtools <integer>
```

New features in FortiOS 5.2.1

This chapter provides a brief introduction to the following features that were added to FortiOS 5.2.1. See the release notes for a complete list of new features/resolved issues in this release.

- Include bandwidth and setup rate statistics in the event log
- Allow export of collected emails
- Ssl-ssh-profile is no longer mandatory when utm profiles are enabled
- Disallow multiple destination interfaces on an IPsec firewall policy
- Add a new diag test command for fnbamd
- Add deregister all option in diagnose endpoint control registration
- Redirect kernel messages to non-console terminals
- Add FortiExtender supported 3G/4G modem list
- Add a new option for STP forwarding
- Suppress probe response based on threshold in wireless controller vap
- Move global antivirus service settings into profile-protocol-options
- Add Ekahau Blink Protocol support and reorganization for station-locate
- Implement diagnose command to test flash SSD
- Online help improvements
- Add iprope check trace in flow trace
- Log id-fields reference improvements
- Add diagnose debug admin error-log command
- Improve hasync debug
- Improve interface list and switch mode
- Wizard improvement
- Allow VIP with port forwarding to permit ICMP
- Support captive portal for block notification page
- Add diagnose log clear-kernel-state command
- Apply new LDAP Tree Browser design to the User Wizard and User Group page
- New Join and try requests to FortiCloud for low-end models

Include bandwidth and setup rate statistics in the event log

Bandwidth and setup rate statistics are vital for customer's units health reports.

The advantage of these parameters are:

- Improves performance on FAZ. Simple query small logs makes FAZ build reports faster and have more idle time for other reports.
- Reduces amount of logs send to FAZ.
- Uses less disk space on FAZ for the same report type.

Allow export of collected emails

This feature adds a new monitor page called **Collected Email Addresses** under **User & Device > Monitor** menu, it is essentially a filter on the device list for devices that have an email address associated with them.

The feature allows the administrator to export the list to a CSV file which can then be used for marketing or analysis purposes.

Ssl-ssh-profile is no longer mandatory when utm profiles are enabled

When UTM profiles are enabled in a security policy, you can set or unset `ssl-ssh profile`.

Syntax

```
config firewall policy
   edit 1
      set ssl-ssh profile <test>
   next
end
```

Disallow multiple destination interfaces on an IPsec firewall policy

When a firewall policy is set to action **IPsec**, multiple **Outgoing Interface** should not be allowed.

Since multiple destination interfaces on an IPsec policy aren't necessary, the CLI and GUI was updated to explicitly disallow it.

Add a new diag test command for fnbamd

The following command was added to show authentication session statistics:

Syntax

```
diagnose test application fnbamd 1
```

Sample output

```
diagnose test application fnbamd 1
Pending sessions:      0
Max session reached:   0
Auth:
   requests:         5000
   sessions:         5000
   released:         5000
Acct:
   requests:         74
   sessions:         0
   released:         0
Cert:
   requests:         0
   sessions:         0
   released:         0
```

Add deregister all option in diagnose endpoint control registration

When there is a long list of registered endpoint needed to be deregistered, the following command was added to do so:

```
diagnose endpoint registration deregister all
```

Redirect kernel messages to non-console terminals

To be able to see kernel messages from ssh or telnet which needed when customer unit is accessible remotely, the following command has been added:

```
diagnose debug application kmiglogd <Integer>
```

`<Integer>` is the debug level. For example, 1 would be the maximum log level in kernel to be shown.

Add FortiExtender supported 3G/4G modem list

A new 3G/4G modem list is introduced that contain the list of supported modems for both FortiGate and FortiExtender.

GUI changes

Under the **System > Network > Modem** page, click **Configure Modem** link under the **External Modem** section to see the list for FortiGate and FortiExtender.

Under the **System > Network > FortiExtender** page, click **Configure Settings** and click **Supported Modems** link under **Modem Settings** section to show the supported FortiExtender modem list. This will jump back to the page under **System > Network > Modem** page, click **Configure Modem** link.

Syntax

The following new diagnose command was added to show the list of supported FortiExtender modems:

```
diagnose extender modem-list
```

Add a new option for STP forwarding

Due to STP forwarding problem in one-arm transparent mode firewall, a new option: replace nothing (`rpl-nothing`) has been added when configuring `stpforward-mode`.

Syntax

```
config system interface
   edit wan1
      set stpforward enable
      set stpforward-mode rpl-nothing
   next
end
```

Suppress probe response based on threshold in wireless controller vap

The wireless controller vap supports probe response suppression (probe-resp-suppression) and probe response threshold (probe-resp-threshold).

Syntax

```
config wireless-controller vap
   edit "SSID"
      set probe-resp-suppression enable|disable
      set probe-resp-threshold <value>
   next
end
```

probe-resp-threshold range is [-20,-95]dBm, and the default is -80dBm if enabled.

Move global antivirus service settings into profile-protocol-options

The global antivirus service settings moved into profile-protocol-options (options included: uncompsizelimit, uncompnestlimit, scan-bzip2, and block-page-status-code). HTTP and HTTPS combined into HTTP, uncompsizelimit changed to uncompressed-oversize-limit and uncompnestlimit to uncompressed-nest-limit. scan-bzip2 set to enabled by default and an appropriate help text added.

On upgrade, the options from antivirus service are moved into the corresponding entries in each profile-protocol-options.

CLI changes

The following options are moved from global antivirus service to firewall profile-protocol-options: uncompsizelimit, uncompnestlimit, scan-bzip2, and block-page-status-code moved.

The following options are removed: ftp, ftps, http, https, imap, imaps, nntp, pop3, pop3s, smtp, and smtps.

The following help test was added:

uncompressed-oversize-limit Maximum in-memory uncompressed size that can be scanned.

uncompressed-nest-limit Maximum uncompress nest level that can be scanned.

scan-bzip2 Enable/disable scanning of BZip2 compressed files.

block-page-status-code Return code of blocked HTTP pages (non-FortiGuard only).

Add Ekahau Blink Protocol support and reorganization for station-locate

We used to have a config command to report station position for retail analytic server under config wireless-controller wtp-profile > radio > station-locate. A new feature ekahua-blink-mode has been added.

These features are all location based service (LBS) related and they moved to a sub-config under wtp-profile, and they are per wtp-profile configuration.

On upgrade, the options from antivirus service are moved into the corresponding entries in each profile-protocol-options.

Syntax

```
config wireless-controller wtp-profile
   edit <wtp-profile-name>
      config lbs
         set ekahau-blink-mode Enable/disable
         set ekahau-tag <xx:xx:xx:xx:xx:xx>
         set erc-server-ip <any_ip>
         set erc-server-port <integer>
      end
end
```

`<xx:xx:xx:xx:xx:xx>` mac address.

`<any_ip>` Any ip xxx.xxx.xxx.xxx.

`<integer>` input integer value.

Implement diagnose command to test flash SSD

A new diagnose command has been implemented to test the disk.

Syntax

```
diagnose disktest <option>
```

Option can be the following:

`device` Specify which device to test.

`block` The block size of each read/write operation.

`time` The limit of test time of each cycles. Default is no limit.

`size` The limit of test size of each cycles. Default is no limit.

`run` Run test with specified cycles. Default is infinite cycles.

Online help improvements

A video links to some help topics has been added in the FortiOS GUI header bar.

Add iprope check trace in flow trace

Previously flow trace shows only accepted or denied policy information. Sometimes, policy tracking is also important and knowing which policies are checked, and what is the result for the checking might be helpful.

Syntax

```
diagnose debug flow show iprope {enable|disable}
```

`enable` to enable trace iprope match.
`disable` to disable trace iprope match.

Log id-fields reference improvements

This improvement is to make a complete reference for each log id with its corresponding fields in FortiOS.

CLI changes

Add new `endpoint` and `ha` subcategories into `config log eventfilter`

Syntax

```
config log eventfilter
   set endpoint Enable/disable
   set ha Enable/disable
end
```

GUI changes

Add subtype log filter options named **Endpoint** and **HA** under **Event Log**

Add diagnose debug admin error-log command

Since the last failed admin login is recorded, this new command shows details about the failed admin login attempt.

Syntax

```
diagnose debug admin error-log
```

Sample output

```
The recent admin user failed login details:
error code       :       -100
method           :       ssh
login name       :       test
cmdb name        :       null
login vdom       :       root
current vdom     :       root
override vdom    :       null
login profile    :       null
override profile :       null
login time       :      2014-08-29 11:01:57
```

Improve hasync debug

Add diag test application hasync to control hasync debug finely.

Syntax

```
diag test application hasync [1-19,50-53]
```

Value	Description
1	Dump all states of debug switches.
2	Turn off all debug switches.
3	Toggle debug switch of hsync core.
4	Toggle debug switch of ha-diff.
5	Toggle debug switch of FIB.
6	Toggle debug switch of route6.
7	Toggle debug switch of BYOD.
8	Toggle debug switch of endpoint_compliance.
9	Toggle debug switch of NEB.
10	Toggle debug switch of zebos.
11	Toggle debug switch of haconf.
12	Toggle debug switch of proxy.
13	Toggle debug switch of time.
14	Toggle debug switch of snmp.
15	Toggle debug switch of gtp.
16	Toggle debug switch of auth.
17	Toggle debug switch of IPsec.
18	Toggle debug switch of fdb.
19	Toggle debug switch of arp.
50	Dump ha sync statistics.
51	Dump FIB information.
52	Dump extfile's signature.
53	Recalculate external files signature.

Improve interface list and switch mode

This features introduces grouping interfaces by interface type and adds switch to toggle between **VLAN Switch Mode** and regular **Hardware Switch Mode**.

GUI changes

- A **Group By Type** toggle switch has been added in the **interfaces** page under **System > Network > Interfaces**.
- A **VLAN Switch Mode** toggle switch has been added in the **interfaces** page under **System > Network > Interfaces**. This **VLAN Switch Mode** toggle switch shows a confirmation dialog when clicked before toggling the system setting.
- A mini faceplate for **Hardware Switch Mode** and **VLAN Switch Mode** has been added in the **member** column under **System > Network > Interfaces**.

Wizard improvement

The Wizard has been improved to provide instruction page to explain how to set up FortiClient for IPsec and SSLVPN and permit to set up FortiCloud connection on Wizard so that logs will be sent to FortiCloud.

GUI changes

- Add instruction module to generate page explaining how to set up FortiClient for IPsec and SSLVPN depending on the VPN that is configured.
- Add a Wizard Summary Page.
- Allow FortiOS Setup wizard to set up FortiCloud.

Allow VIP with port forwarding to permit ICMP

When a VIP is defined with port forwarding enabled, ICMP (PING) to the mapped IP can be allowed.

Syntax

```
config firewall vip
   edit "VIP"
      set extip xxx.xxx.xxx.xxx
      set extintf "wan1"
      set portforward enable
      set mappedip xxx.xxx.xxx.xxx
      set protocol icmp
   next
end
```

The command `set protocol` has `icmp` option now to make the firewall forward ICMP to the host specified by `mappedip` while the `mappedport` and `extport` attributes are skipped.

Support captive portal for block notification page

The main requirement of this feature is to present a block notification page if the web access is denied by a firewall policy.

Add diagnose log clear-kernel-state command

This command has been added to clear log statistics in kernel in order to improve disk log session setup rate.

Syntax

```
diagnose log clear-kernel-stats
```

Apply new LDAP Tree Browser design to the User Wizard and User Group page

Previously, the LDAP browser shows LDAP containers and LDAP entries within the same tree. When there are many LDAP entries available, it becomes harder for users to select, filter, search different types of LDAP objects.

This new feature now divides the LDAP Browser into two major parts:

- A tree to show the container.
- Tables to show different type of LDAP object entries.

New Join and try requests to FortiCloud for low-end models

These new `join` and `try` requests are for low-end models only such as: FG-30D, FWF-30D, FG-60D, FWF-60D, FG-70D, FG-80D, FG-90D, and FWF-90D.

Syntax

```
exec fortiguard-log join
exec fortiguard-log try <FortiCloud_id> <Password>
```

Top Features

This chapter introduces the following top features of FortiOS 5.2:

- Unified Policy Management
- FortiView Dashboards
- SSL Inspection
- Web Filtering
- Application Control
- IPsec VPN Creation Wizard
- Captive Portal
- FortiAP Management
- Flow-based Antivirus
- FortiExtender Support
- Using a Virtual WAN Link for Redundant Internet Connections
- Internet Key Exchange (IKE)
- SSL VPN Creation
- On-Net Status for FortiClient Devices

Unified Policy Management

The different creation pages in the web-based manager for policy types and subtypes (user-identity, device identity, and VPN) have been merged into a single main policy creation page. New fields have been added for **Source User(s)** and **Source Device Type** that remove the need for multiple authentication rules in a single policy. This allows for greater control and customization of policies, as a combination of these source types can be used in a single policy rather than having to pick one type.

For more information, see Unified Policy Management on page 103.

FortiView Dashboards

The **FortiView** dashboards integrate real time and historical dashboards into a single view that displays the top 100 sessions on a FortiGate unit. The different dashboards show information on the following:

- Sources
- Applications
- Cloud applications
- Destinations
- Web sites
- Threats
- All sessions

For more information, see "Usability Enhancements" on page 92.

SSL Inspection

Several changes have been made to how SSL inspection is handled by a FortiGate unit, with the addition of a new mode that allowed HTTPS traffic to be scanned without enabling deep inspection, as well as changes to the handling of certificates and configuring exemptions for SSL inspection.

For more information, see SSL Inspection on page 114.

Web Filtering

Several new options have been added for web filtering:

- Restricting Google access to specific domains
- New protocols for warnings and authentication
- Modifying HTTP request headers
- Adding a referer to URL filters.
- Using FortiGuard rating checks for images, JavaScript, CSS, and CRL
- Additional replacement message variables

For more information, see Web Filtering on page 116.

Application Control

Several new options have been added for application control:

- Deep inspection for cloud applications
- Traffic shaping settings
- 5-Point-Risk Ratings
- Replacement messages
- Support for SPDY protocol

For more information, see "Security Profiles" on page 119.

IPsec VPN Creation Wizard

The IPsec VPN wizard is the only web-based manager tool for creating interface- or route-based IPsec VPNs. All it takes is a few steps with the wizard to create a wide variety of interface-based IPsec VPN configurations. In addition to the IPsec settings the wizard creates all required routes and policies.

In FortiOS 5.2, expanded options have been added to the wizard, allowing it to be used for more types of VPN configurations. Tunnel templates have been created for popular configurations.

For more information, see VPN Creation Wizard on page 124.

Captive Portal

Several new options have been added for captive portals:

- External captive portals
- Using groups from the security policy

- Exempting a policy
- Replacement messages
- New configuration options for wireless
- WPA personal security + captive portal for wireless

For more information, see Captive Portal on page 134 and Captive Portal for WiFi on page 142.

FortiAP Management

Several new options have been added for managing FortiAP units:

- Manually selecting AP profiles
- AP scanning
- Radio settings summary
- CLI console access
- Split tunneling for wireless traffic

For more information, see FortiAP Management on page 140.

Flow-based Antivirus

In FortiOS 5.2, flow-based AntiVirus has been improved to have the same enhanced performance as flow-based antivirus scanning in FortiOS 5.0 while providing the same accuracy and many of the extended features of proxy-based antivirus.

For more information, see Flow-based Antivirus on page 121.

FortiExtender Support

FortiOS 5.2 supports FortiExtender, that allows you to remotely connect 4G/LTE USB modems to a FortiGate unit. The FortiGate unit can remained installed in a secure location while the FortiExtender is installed on a roof or near a window providing enhanced 4G/LTE modem reception.

For more information, see FortiExtender Support on page 76.

Using a Virtual WAN Link for Redundant Internet Connections

A virtual WAN link consists of two or more interfaces that are connected to multiple ISPs. The FortiGate unit sees the virtual WAN link as a single interface so the FortiGate's security policy configuration no longer has be redundant to support dual Internet links. In addition, the virtual WAN link includes load balancing and new link health checking and settings.

For more information, see Using a Virtual WAN Link for Redundant Internet Connections on page 78.

Internet Key Exchange (IKE)

Several new options have been added for how IKE is supported on a FortiGate:

- Multiple interfaces
- Mode-configuration
- Certificates groups

- Authentication methods
- Inheriting groups from the security policy
- Assigning client IP addresses using the DHCP proxy
- Transform matching
- Cookie notification
- Message ID sync for High Availability

For more information, see Internet Key Exchange (IKE) on page 126.

SSL VPN Creation

SSL VPN configuration has been simplified with new settings and portal creation pages. Most SSL VPN settings can be configured on one web-based manager page, with additional settings handled as part of the security policy.

For more information, see SSL VPN Configuration on page 132.

On-Net Status for FortiClient Devices

A new status option, On-Net, has been added for FortiClient devices that show if that device has been registered with the FortiGate unit.

For more information, see On-Net Status for FortiClient Devices on page 138.

System Features

New system features include:

- FortiExtender Support
- Using a Virtual WAN Link for Redundant Internet Connections
- FortiGuard Services
- Netflow v9.0
- DHCP Server Configuration
- Improvements to Aggregate/Redundant Interfaces
- Link Layer Discovery Protocol
- CPU and Memory Usage per VDOM
- Custom Languages for Guest Management and SSL VPN Portals
- Packet Capture Options for Admin Profiles
- FortiCloud Modem List
- SPAN Support for Hard-Switch Interfaces
- Setting the Service and AC-name in PPOE PADI/PADO Negotiations
- Disabling FortiExplorer, the USB MGMT Port, and the Serial Console
- Port Kernel Profiling
- Using a Second Destination IP (VRDST)
- Session Rate Stats per VDOM
- Disable Honoring the Don't-Fragment Flag
- Disable Login Time Recording
- Per-IP-Bandwidth-Usage Feature Removed
- Modem Support

FortiExtender Support

FortiOS 5.2 supports the new FortiExtender unit, which provides internet connectivity via 4G/LTE network to a FortiGate unit.

To connect a FortiGate and FortiExtender, a new tap interface is created on the FortiGate unit, which receives the IP address from the cellular service provider via the FortiExtender, using a CAPWAP data channel. All the packets sent to the tap interface are received by the extender module on the FortiGate and are then sent to the FortiExtender, which then sends the packets out on the 4G/LTE network.

When data packets are received from the cellular network, the FortiExtender passes the packets to the FortiGate via the CAPWAP data channel. These packets are written to the tap interface and the FortiGate IP stack will process them.

The options to configure a FortiExtender unit can be found by going to **System > Network > FortiExtender**.

The configuration of a FortiExtender interface is restricted to the root VDOM.

Connecting a FortiExtender unit to a FortiGate unit

1. If you are using the provided PoE injector:
   a. Plug the provided Ethernet cable into the Ethernet port of the FortiExtender and insert the other end of the Ethernet cable into the AP/Bridge port on the injector, then plug the injector into an electrical outlet.
   b. Connect the LAN port of the PoE injector to a FortiGate, FortiWifi, or FortiSwitch device.
2. If you are not using the PoE injector, insert the other end of the Ethernet cable into a PoE LAN port on an appropriate FortiGate, FortiWiFi or FortiSwitch device.
3. By default, the options for the FortiExtender are hidden and disabled. Enable them in FortiGate's CLI:

```
config system global
   set fortiextender enable
   set wireless-controller enable
end
```

4. Enable the control and provisioning of Wireless Access Point (CAPWAP) service on the port to which the FortiExtender unit is connected (**lan** interface in this example) using the following CLI commands:

```
config system interface
   edit lan
      set allowaccess capwap
   end
end
```

Once enabled, it appears as a virtual WAN interface in the FortiGate, such as *fext-wan1*.

Configuring the FortiExtender unit

1. At this point, you can fully manage the FortiExtender from the FortiGate unit. To achieve this, you need to authorize the FortiExtender by going to **System > Network > FortiExtender** and click on **Authorize**. Once authorized, you can configure the following settings as required:
   - **Link Status**: Shows you if the link is **Up** or **Down**, click on **Details** to see the System and Modem Status.
   - **IP Address**: Shows you the current FortiExtender's IP address, click on the link of the IP address to connect to the FortiExtender GUI.
   - **OS Version:** Shows the current FortiExtender's build, click on **Upgrade** if you wish to upgrade the Firmware.
   - **Configure Settings**: Allows you to configure the Modem Settings (for more information, see below), PPP Authentication, General, GSM / LTE, and CDMA .
   - **Diagnostics**: Allows you to diagnose the FortiExtender unit, you can choose a command form the existing commands and click on **Run**. Existing commands are: `Show device info, Show data session connection status, test connection, test disconnection, Get signal strength, AT Command.`

The FortiExtender unit allows for two modes of operation for the modem; **On Demand** and **Always Connect**. In **On Demand** mode, the modem connects to a dialup ISP account to provide the connection to the Internet when needed. In **Always Connect** mode, the modem is always connected to the internet, it can acts as a primary or backup method of connecting to the Internet. To configure the dial mode as needed, do the following:

2. Select **Configure Settings**.
3. Extend **Modem Settings**.
4. Select the **Dial Mode** of **Always Connect** or **On Demand**.
5. Enter the **Quota Limit** to the desired limit in Mega Byte.
6. Select **OK**.

Configuring the FortiGate unit

1. Go to **Router > Static > Static Routes** or **System > Network > Routing**, depending on your FortiGate model, and select **Create New**.

If your network will be using IPv6 addresses, go to **Router > Static > Static Routes** or **System > Network > Routing** and select **IPv6 Route**.

2. Set the **Destination IP/Mask** to 0.0.0.0/0.0.0.0, **Device** to **fext-wan1**, and set the **Gateway** to your gateway IP or to the next hop router, depending on your network requirements.
3. Select **OK.**
4. Go to **Policy & Objects > Policy > IPv4** and select **Create New.**

If your network will be using IPv6 addresses, go to **Policy & Objects > Policy > IPv6** and select **Create New.**

5. Set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to **fext-wan1** interface. You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements.
6. Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected.
7. Select **OK.**

Using a Virtual WAN Link for Redundant Internet Connections

To make sure your network is always connected to the Internet you can engage the services of two or more Internet service providers and set up redundant Internet connections. Then, if one of your ISPs service is interrupted, all of your Internet traffic can be switched to the other ISP, maintaining your Internet connection. Also, while both ISPs are operating you can load balance traffic between them, increasing your network's available Internet bandwidth.

Previous versions of FortiOS required a few steps to set up two interfaces as redundant Internet connections. The setup also involved some special routing and load balancing setup and creating duplicate policy configurations for each Internet facing interface. In addition, previous versions of FortiOS supported basic link monitoring.

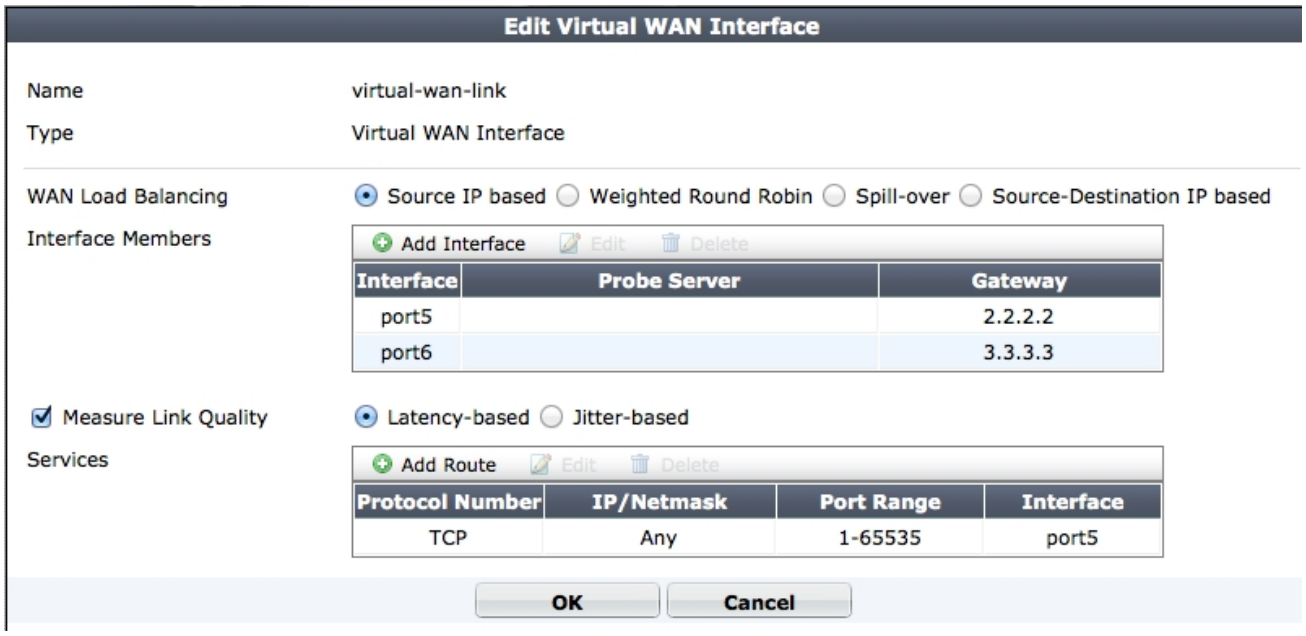
FortiOS 5.2 adds a new type of interface called a virtual WAN link. A virtual WAN link consists of two or more physical interfaces that are connected to two or more ISPs and to the Internet as well as the load balancing and routing configuration required to support redundant internet connections. In addition, the virtual WAN link configuration also includes new link health checking and settings to control traffic flow based on link health.

The FortiGate unit sees the virtual WAN link as a single interface so the FortiGate's security policy configuration no longer has be redundant to support dual Internet links. Now one policy configuration to control traffic to the virtual WAN link is all that is required. You can also add or remove redundant Internet links just by adding or removing physical interfaces from the virtual WAN link. No addition changes to the routing, load balancing or firewall policy configuration are required.

Setting Up a Virtual WAN Link

To set up a virtual WAN link, go to **System > Network > Interfaces** and select **Create New > Virtual WAN**. Add the interfaces connected to ISPs to the virtual WAN link. For each interface you must enter a gateway IP, usually provided by your ISP. You can also change load balancing settings (such as Spillover Threshold and Weight) and set up link health checking (called measuring link quality).

Virtual WAN link configuration



Once you have added interfaces to the virtual WAN interface you should go to **Router > Static > Static Route** and add a default route for the virtual WAN link. Then add firewall policies that allow access to the Internet by setting the outgoing interface to virtual-wan-link.

For more information about using a virtual WAN link, please see the FortiGate Cookbook recipe Redundant Internet connections (5.2.0) .

Setting Up Virtual WAN Link Load Balancing

By default when you set up a virtual WAN link source IP based load balancing is selected and traffic is load balanced among the interfaces added to virtual WAN link configuration. You can change the load balancing method to weighted load balancing, spill-over load balancing or source-destination IP load balancing. Selecting a different load balancing method may also require configuring the interfaces added to the virtual WAN link to add weights (for weighted load balancing) or to set spillover thresholds.

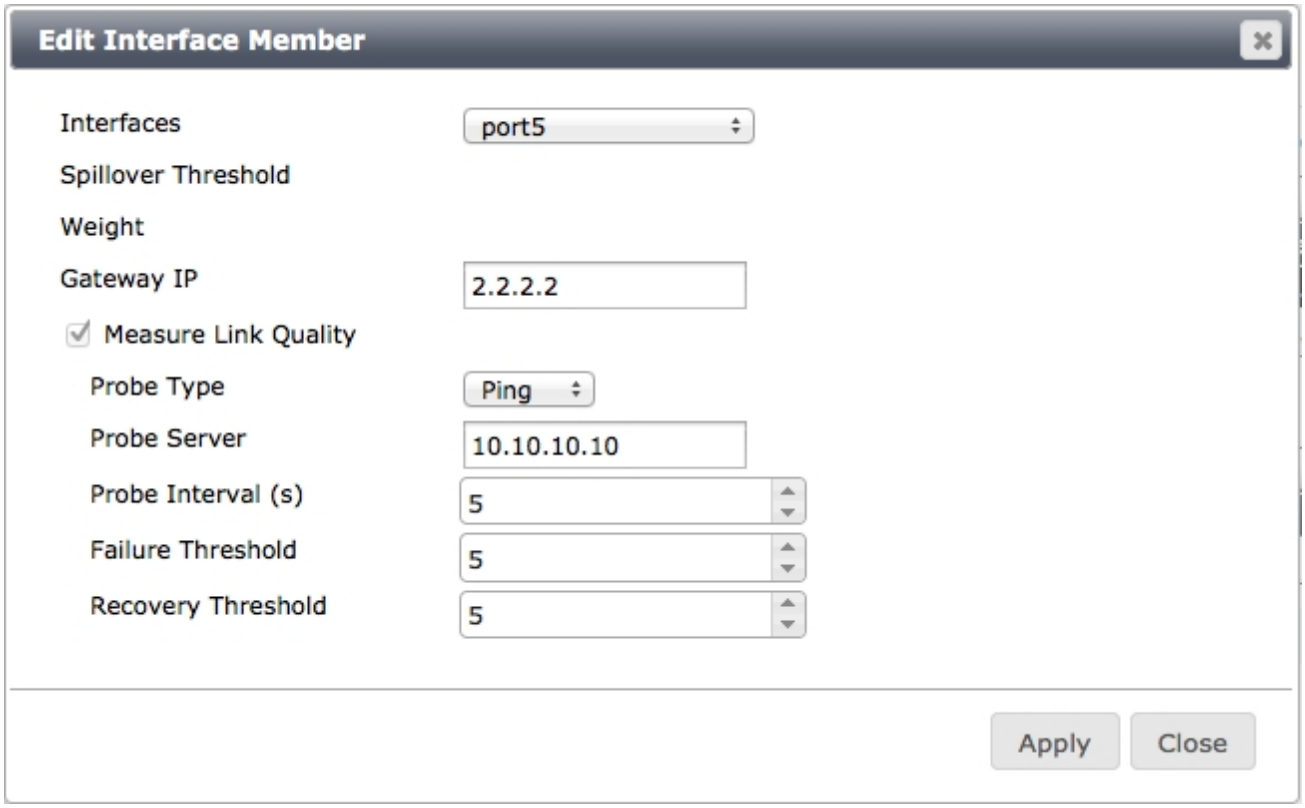
Directing Traffic to Higher Quality Links

You can configure link quality measuring (link health checking) on the interfaces added to the virtual WAN link. Depending on how you configure the virtual WAN link this link quality checking is based on latency or jitter. With link quality checking in place you can configure Services to control the links used for selected types of traffic. For example, media-based traffic like SIP is very sensitive to jitter. If you set up link quality checking to check for jitter,

you can configure the virtual WAN link to send SIP traffic to the link with the lowest jitter (and so the highest quality link).

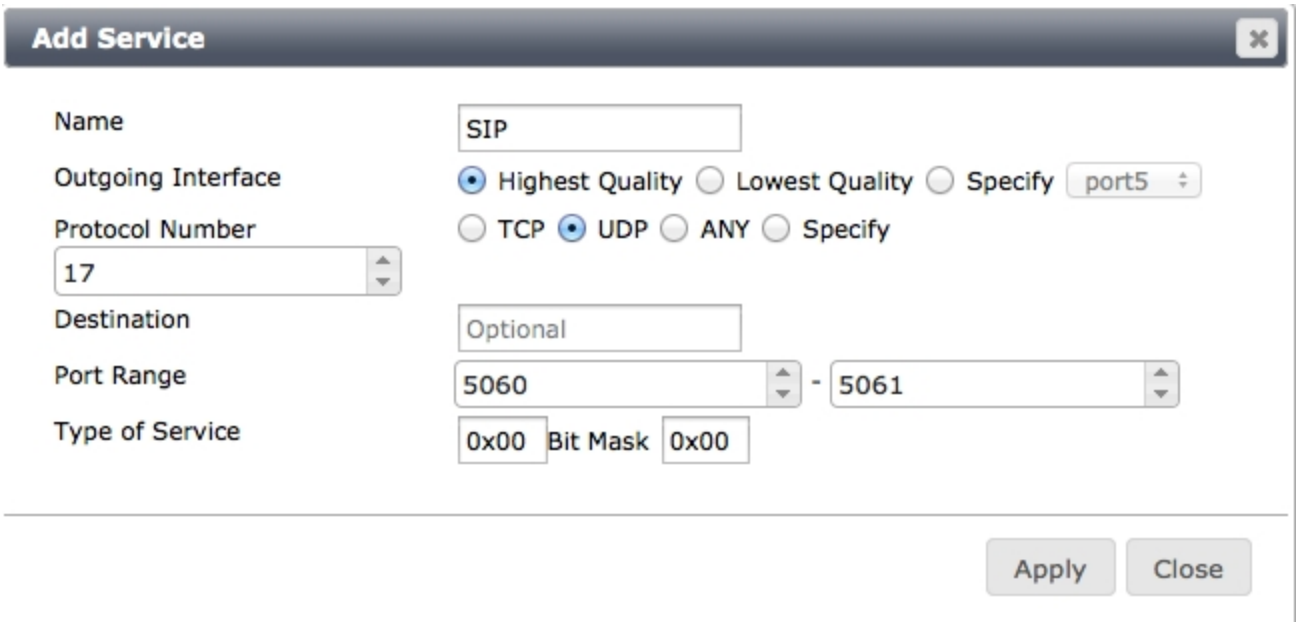
To configure link checking on individual interfaces added to a virtual WAN link, edit Interface members in the virtual WAN link, select Measure Link Quality and set the quality measurement options. You can measure link quality using ping or HTTP, select a server to communicate with to perform link quality checking and set the probe interval, failure threshold and recovery threshold.

Configuring link health checking



Next, add Services that control how traffic patterns are affected by link quality. Services work like policy routes. Configure a service by defining a traffic type (for example, SIP) and specifying whether this traffic always goes to the highest quality interface, the lowest quality interface or a specific interface no matter the quality.

Virtual WAN link service



Measured Volume Based Distribution

Your FortiGate can actively measure the volume of traffic sent to each WAN link and distribute new sessions to balance the traffic volume to each link using a simple ratio calculation. To use this feature, use the following CLI command:

```
config system virtual-wan-link
   set load-balance-mode measured-volume-based
   config member
      edit <ID>
         set volume-ratio <number>
      end
   end
end
```

The Link Monitor

You can monitor link health using the **Link** monitor, which can be found by going to **System > Monitor > Link Monitor**.

FortiGuard Services

Several changes have been made to how FortiGuard services can be received by your FortiGate unit.

FortiGuard Server List

In FortiOS 5.2, you can create a server list for receiving FortiGuard updates, allowing you to use different servers for different FortiGuard services. Each server can be used for either web filter and anti-spam ratings or AV/IPS signature updates.

The server list also has the ability to include the default servers by adding them to the end of the list. This option is only available if the central management type is not set to FortiGuard.

If no server list is configured, the FortiGuard will not use the public FortiGuard servers as resolved by DNS.

Syntax

```
config system central-management
   config server-list
      edit <ID>
         set server-type {rating | update}
         set server-address <address>
      end
   set include-default-servers {enable | disable}
end
```

Using TCP Port 80 to Receive Updates from a FortiManager Unit

Communications to a FortiManager unit in order to receive FortiGuard updates are now supported using TCP port 80.

To configure communications to use port 80, go to **System > Config > FortiGuard** and expand **Web Filtering and Email Filtering Options**. Select **Use Alternate Port (80)**. This can also be configured using the CLI.

Syntax

```
config system fortiguard
   set port 80
end
```

FortiGuard TCP stats can also be displayed using the `diagnose test application urlfilter 20` command.

Netflow v9.0

FortiOS 5.2 supports Netflow v9.0. NetFlow services provide network administrators with access to IP flow information from their data networks. Network elements (routers and switches) gather flow data and export it to collectors. The collected data provides fine-grained metering for highly flexible and detailed resource usage accounting.

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flow records include details such as IP addresses, packet and byte counts, timestamps, application ports, and input and output interfaces.

Configuring the Global Settings for Netflow Collector and Timers

The global settings for Netflow can be configured in the CLI:

```
config system netflow
   set collector-ip <address>
   set collector-port <port>
   set source-ip <address>
   set active-flow-timeout <integer>
   set inactive-flow-timeout <integer>
end
```

The value for `active-flow-timeout` is used as the minimum length of a live session, as well as for the intervals to send the report. The default is 1 minute, meaning that if a session lives for a minute, it will be reported in a Netflow packet.

The value for `inactive-flow-timeout` is used as the interval to send a Netflow report of inactive (finished) flows. Since FortiOS uses 1350 Byte payloads, the number of reports in a packet are limited and multiple packets may be sent regardless of this timer.

Using Netflow with VDOMs

For VDOM environments, excluding the management VDOM, Netflow must be configured using the following CLI commands:

```
config system vdom-netflow
   set vdom-netflow enable
   set collector-ip <address>
   set collector-port <port>
   set source-ip <address>
end
```

Adding Netflow Sampling to an Interface

Netflow sampling can be enabled on an interface to sample transmitted traffic (tx), received traffic (rx), or both using the CLI:

```
config system interface
   edit <name>
      set netflow-sampler {disable | tx | rx | both}
   end
end
```

Viewing the Configuration

Netflow does not have a separate daemon and is instead running under sflowd. The current Netflow configuration can be viewed by using test level 3 or 4:

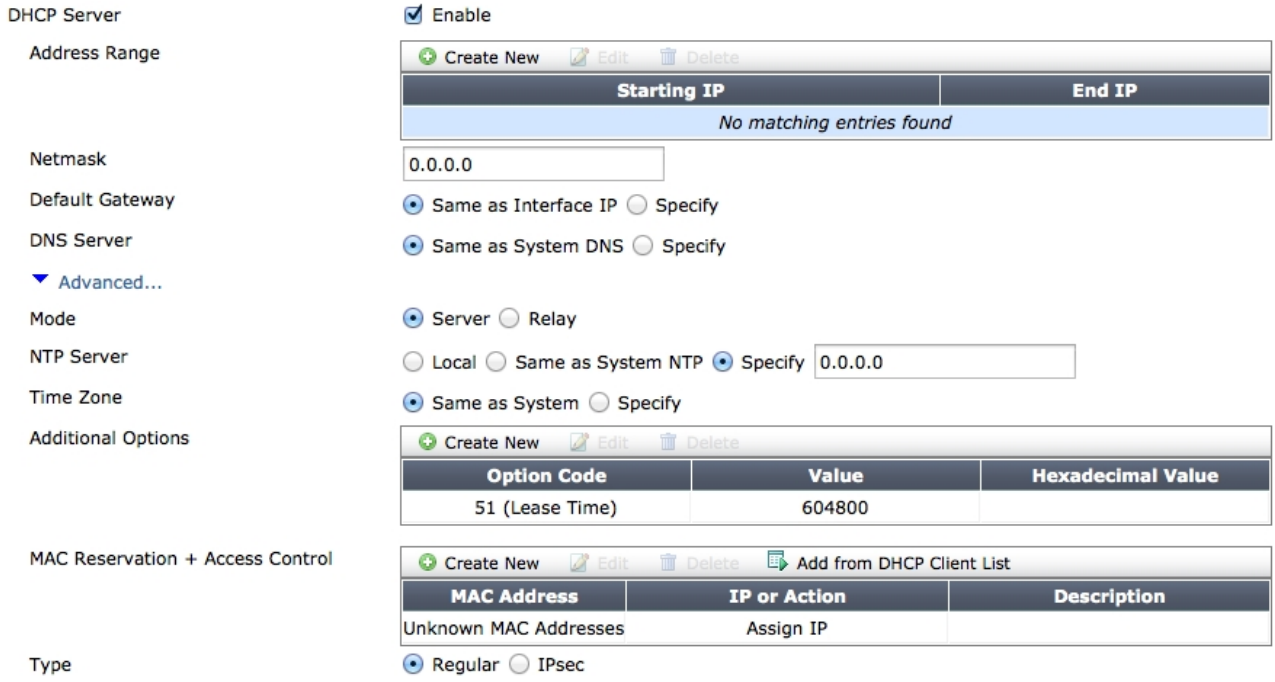
```
diagnose test application sflowd 3
diagnose test application sflowd 4
```

DHCP Server Configuration

The following attributes have been added for DHCP server configuration to both the web-based manager and the CLI:

- Time zone
- TFTP server
- TFTP filename

DCHP server settings



Syntax

```
config system dhcp server
   edit <integer>
      set timezone-option {disable | default | specify}
      set timezone <timezone_code>
      set tftp-server <string>
      set filename <file_name>
   end
end
```

Improvements to Aggregate/Redundant Interfaces

Several improvements have been made in FortiOS 5.2 for aggregate or redundant interfaces.

Minimum Number of Links in an Aggregation

You can now set a minimum number of links that must exist in an aggregation. If this number is not reached, the device will failover. The minimum links value can be set between 1-32, with 1 being the default value.

Aggregates can also now be configured so that they are taken down administratively when the min-links threshold is passed. This will cause all the members to be taken down administratively as well.

Syntax

```
config system interface
   edit <name>
      set type aggregate
      set vdom root
      set member <ports>
      set min-links <integer>
      set min-links-down administrative
   end
end
```

Avoiding Traffic Disturbances

Two new methods have been added to avoid traffic disturbances for an aggregate that can be caused by ports flapping up and down and being repeatedly added and removed from the aggregate.

Setting the Link Up Delay Period

When a member port in an aggregate/redundant becomes operationally up, be default it is considered as a viable port for aggregation/redundancy after 50ms. Increasing this delay can minimizing the effect of a flapping port by causing the FortiGate to wait longer before deciding if a port is considered viable. This option is available for both redundant and aggregate interfaces.

Syntax

```
config system interface
   edit <name>
      set type {aggregate | redundant}
      set link-up-delay <time>
   end
end
```

Enabling Priority Override

In the case of a redundant port, there is only one port actively carrying traffic thus the only time a port coming up can affect existing traffic is where the primary port went down, traffic moved to a secondary and then the primary came back up. In this case since there is only one port the impact of switching ports is more noticeable and thus it may be desirable to not switch back to the original primary just because it is up. Instead traffic should only switch back if the currently active secondary fails.

To support that, the command `set priority-override` has been added for redundant interfaces. If `priority-override` is enabled, then when a port with a higher priority comes up then traffic switches to it. With `priority-override` disabled, traffic will only switch to a higher priority port if the current port fails.

Syntax

```
config system interface
   edit <name>
      set type redundant
      set priority-override {enable | disable}
   end
end
```

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is supported in FortiOS 5.2. LLDP allows a device to advertise its existence and capabilities to other devices.

The primary use for LLDP is to improve a FortiGate unit's device detection output when another FortiGate unit is detected. LLDP information is used to populate the device record on the FortiGate unit performing device detection. Any LLDP information transmitted by a peer is ignored unless FortiGate device detection is enabled on an interface. If device detection is enabled, then the subset of LLDP information sent by the peer that is relevant to device detection is shown in the `diagnose user device list` output.

The transmitted LLDP attributes on a given port are:

- Chassis ID
- Port ID
- TTL
- System Name
- System Description
- System Capabilities
- Aggregation
- Host Name

LLDP transmission is enabled by default on all ports that support a MAC address. It can be disabled globally, or disabled on some interfaces or VDOMs, while being enabled on others.

Syntax

To disable LLDP globally or on a specific VDOM, use the following command:

```
config system global
   set lldp-transmission disable
end
```

To enable LLDP at the individual interface level, first disable LLDP globally, then use the following command:

```
config system interface
   edit <name>
      set lldp-transmission enable
   end
end
```

CPU and Memory Usage per VDOM

In FortiOS 5.2, the following information sources are available concerning both CPU and memory usage per VDOM:

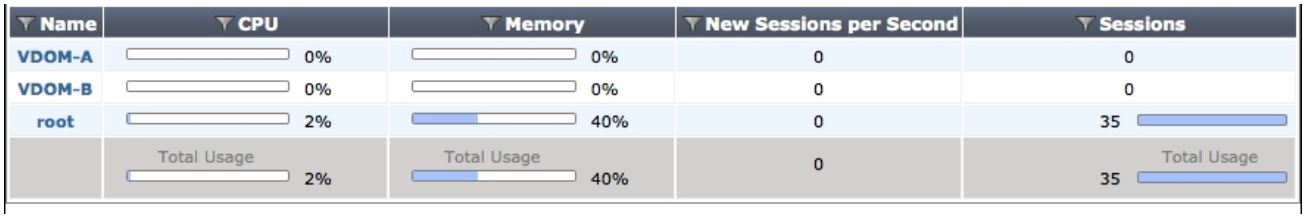
Default columns for CPU and Memory have been added to the VDOM list.

Optional columns for Sessions and New Sessions per Second have been added to the VDOM list.

A summary line has been added to at the bottom of the VDOM list to show global CPU, memory, sessions, and sessions per second usage.

The CLI command `diagnose sys vd stats` has been added to display VDOM statistics.

VDOM list



Custom Languages for Guest Management and SSL VPN Portals

Custom language files can now be used for guest management admin accounts, as well as guest portals, SSL VPN portals, and SSL VPN user settings.

To use this feature, it must be enabled in the CLI. Language files can now be managed, imported, and downloaded by going to **System > Config > Advanced**. Further configuration can be done in the CLI.

Syntax

1. Enabling the feature:

```
config system global
   set gui-custom-language enable
end
```

2. Downloading a custom language file from a TFTP server:

```
execute system custom-language import <lang_name> <file_name> <tftp_server_ip>
```

3. Managing custom languages:

```
config system custom-language
   edit <lang_name>
      set filename <file_name>
   end
end
```

4. Setting the custom language for an admin account with `guest-auth` enabled:

```
config system admin
   edit <name>
      set guest-auth enable
      set guest-lang <lang_name>
   end
end
```

5. Setting the custom language for an SSL-VPN portal with `web-mode` enabled:

```
config vpn ssl interface
   edit <name>
      set web-mode enable
      set custom-lang <lang_name>
   end
end
```

6. Setting the custom language for an SSL-VPN user:

```
config vpn ssl web user-bookmark
   edit <name>
      set custom-lang <lang_name>
   end
end
```

Packet Capture Options for Admin Profiles

Packet capture can now be configured in an admin profile and set to **None**, **Read Only**, or **Read-Write**. The packet capture option can be found by going to **System > Admin > Admin Profiles** and expanding **Firewall Configuration**.

This feature can also be configured in the CLI.

Syntax

```
config system accprofile
   edit <name>
      set fwgrp custom
         config fwgrp-permission
            set packet-capture {read-only | read-write | none}
         end
      end
end
```

FortiCloud Modem List

The supported modem list that can be downloaded from FortiCloud will now include a list of supported modems by FortiOS and the new FortiExtender unit. To support this, the file format of the list changed from plain text to tar ball that contains two files: `modem_list.conf` for the FortiOS list and `modem_list_fex.conf` for the FortiExtender list.

SPAN Support for Hard-Switch Interfaces

The Switch Port Analyzer (SPAN) feature is now available for hardware switch interfaces on FortiGate models with built-in hardware switches (for example, the FortiGate-100D, 140D, and 200D etc.). The SPAN feature (also called port mirroring) allows you to send a copy of the packets received or sent by one interface to another. So, for example, you could send all traffic received by the WAN interface to another interface and connect a sniffer to that other interface to monitor the traffic on the WAN interface.

To enable SPAN on a hardware switch, go to **System > Network > Interfaces** and edit a hardware switch interface. By default the system may have a hardware switch interface called **lan**. You can also create a new hardware switch interface.

Select the **SPAN** checkbox. Select a source port from which traffic will be mirrored. Select the destination port to which the mirrored traffic is sent. Select to mirror traffic received, traffic sent, or both.

Configuring SPAN

You can also enable SPAN in the CLI:

Syntax

```
config system virtual-switch
   edit <port>
      set span enable
      set span-source-port <port>
      set span-dest-port <port>
      set span-direction {both | Tx | Rx}
   end
end
```

Setting the Service and AC-name in PPOE PADI/PADO Negotiations

The Service and AC name in the PPPoE PADI/PADO negotiation is now configurable. This allows CLI-specified names to encoded, enhancing logic in the handling of various PPPoE server responses, especially in situations where there are multiple Access Concentrator servers in the Point of Presence site.

Syntax

```
edit port1
   set mode pppoe
   set service-name <name>
   set ac-name <name>
end
```

Disabling FortiExplorer, the USB MGMT Port, and the Serial Console

New CLI commands have been added allowing you to disable access for FortiExplorer on Windows and OS X and the USB MGMT port, or for the serial console, FortiExplorer iOS, the USB MGMT port, and 3G/4G MODEM access.

Syntax

1. Disable FortiExplorer on Windows and OS X and the USB MGMT port:

```
config system console
   set fortiexplorer disable
end
```

2. Disable serial console, FortiExplorer iOS, and 3G/4G MODEM access:

```
config system console
```

```
        set login disable
    end
```

Port Kernel Profiling

Port kernel profiling is now supported in FortiOS 5.2. To use this feature, enter the command `diagnose sys profile` into the CLI. If you press enter, the following options are available:

1. set cpu mask
2. run start command
3. run stop command to read the profiling data and analyze
4. run show command to show the result
5. set cpu mask 00 to stop profiling

The following attributes are also available:

- `cpumask` - profile which CPUs.
- `module` - show kernel module (This is only available when the kernel is module mode).
- `show` - show kernel profiling result.
- `start` - start kernel profiling data.
- `stop` - copy kernel profiling data.
- `sysmap` - show kernel sysmap.

Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down.

A second VRDST can be configured using the CLI.

Syntax

```
config system interface
   edit <interface>
      config vrrp
         edit <id>
            set vrdst <ip1> <ip2>
         end
      end
end
```

Session Rate Stats per VDOM

The command `diagnose sys vd list` now displays the session setup rate. This feature is supported for both IPv4 and IPv6.

Disable Honoring the Don't-Fragment Flag

Honoring the Don't-Fragment flag can now be disabled through the CLI. This allows the FortiGate unit to fragment the packet as required, even when the Don't-Fragment flag is set.

Syntax

```
config system global
   set honor-df disable
end
```

Disable Login Time Recording

Login time recording, which is enabled by default, can now be disabled using the CLI.

Syntax

```
config system global
   set login-timestamp disable
end
```

Per-IP-Bandwidth-Usage Feature Removed

The Per-IP-Bandwidth feature has been removed in FortiOS 5.2. This includes both the **Per-P-Bandwidth** widget in the web-based manager and all related CLI commands.

Modem Support

The Novatel MC679 and Sierra 313U modems are supported in FortiOS 5.2 for use with a FortiGate unit.

An MIB entry, `fgUsbModemSignalStrength`, has also been added to display modem signal strength.

Usability Enhancements

Many usability enhancements have been made to the web-based manager in FortiOS 5.2, in order to make the configuration process more efficient. New usability enhancements include:

- FortiView Dashboards
- FortiExplorer Setup Wizard Improvements
- Interfaces List Improvements
- Dragging Objects Between Policies in the Policy List
- Cloning Table Objects
- DHCP-related Improvements in the Web-based Manager
- System Resources Widget
- License Information Widget
- USB Modem Widget
- New Feature Settings Preset
- Improved Banned User List Page
- Replacement Message Improvements
- Sorting and Filtering Support for the Virtual IP list
- Web-based Manager Options for the FortiGate-30D

FortiView Dashboards

In order for information to appear in the **FortiView** dashboards, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Config > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

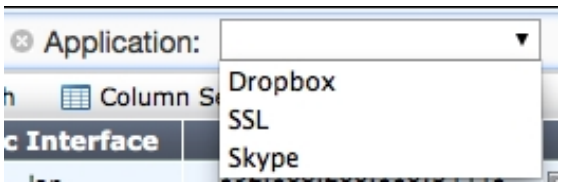
```
config log disk setting
     set status enable
end
```

Please note that flash-based logging has been disabled in FortiOS 5.2 for certain models. To view a complete list of affected models, please refer to the Release Notes.

The **FortiView** dashboards integrate real time and historical dashboards into a single view. These dashboards can be found by going to **Status > FortiView**. Each dashboard will initially display the top 100 sessions but when the results are filtered, other sessions may be displayed.

Each dashboards can be filtered by a variety of attributes. Attributes can be selected by using the dropdown menu located at the top of each widgets that displays only the options that have results; for example, if the only applications used in the are Dropbox, SSL, and Skype, the only options in the dropdown menu for the Application filter will be Dropbox, SSL, and Skype.

Filtering for Applications



Results can also be filtered using the various columns, although not all columns support this.

The dashboards also include different time options, allowing you to see current traffic in real-time, or historical traffic that occurred in the last 5 minutes, 1 hour, or 24 hours.

Historical traffic is only supported on FortiGate models that have local storage. The 24 hours option is also unavailable for desktop models (FortiGate-90 series and below).

Sources

The **Sources** dashboard shows information about the sources of traffic on your FortiGate unit, including user and device. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by source IP, source device, source interface, destination interface, and policy ID.

The Sources dashboard

Source	Device	Sessions	Bytes (Sent/Received)
10.10.80.3	Alais	122	539.94 K
10.10.80.4	Nicola	4	163.12 K
10.10.80.2	Wii	1	386

Applications

The **Applications** dashboard shows information about the applications being used on your network, including application name, category, and risk level. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the **Applications** dashboard, application control must be enabled in a policy.

The Applications dashboard

Application	Category	Risk	Sessions	Bytes (Sent/Received)
DNS	Network.Service		35	9.44 K
Skype	P2P		23	589.99 K
Hola.Unblocker	Proxy		21	440.08 K
SMTPS	Email		1	10.46 K
Dropbox	Storage.Backup		1	12.11 K

Cloud Applications

The **Cloud Applications** dashboard shows information about the cloud applications being used on your network, including application name, category, risk level, login IDs, and, if applicable, the number of videos played. If the cursor is held over the column showing the number of videos, the titles of these videos will be shown. Additional columns show information about sessions and bytes sent or received.

Two different views are available for the Cloud Applications dashboard: applications and users. Applications shows a list of the programs being used. Users shows information on the individual users of the cloud applications, including the username if the FortiGate was able to view the login event.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the **Cloud Applications** dashboard, an application control profile that has **Deep Inspection of Cloud Applications** turned on must be enabled in a policy and SSL Inspection must use `deep-inspection` (for more information, see "SSL Inspection").

The Cloud Applications dashboard

Application	Category	Risk	Login IDs	Sessions	Files (Up/Down)	Videos Played	Bytes (Sent/Receive
Youtube	Video/Audio		1	25		8	139.77 M
Vimeo	Video/Audio		1	1		1	4.85 M
Dropbox	File.Sharing		1	1	0 / 1		15.09 M

Destinations

The **Destinations** dashboard shows information about the destination IPs of traffic on your FortiGate unit, as well as the application used. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by destination IP, user, source interface, destination interface, and policy ID.

The Destinations dashboard

Destination	Applicati...	Sessions	Bytes (Sent/Received)
pongs.blip.tv (54.243.171.49)	Unknown	2	71.42 K
gwb.lphbs.com (199.127.194.181)	Unknown	1	45.33 K
notify3.dropbox.com (108.160.167.157)	Dropbox	1	555
dsn0.d.skype.net (157.55.130.156)	Unknown	1	8.29 K
dsn15.d.skype.net (157.55.56.154)	Unknown	1	3.84 K
104.0.14.6.0.rst6.r.skype.net (157.55.133.145)	Unknown	1	5.03 K

Websites

The **Websites** dashboard lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be clicked on in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand. New icons have also been added for FortiGuard category groups. Additional information is provided about domain, browsing time, threat weight, sources, and bytes sent or received.

This dashboard can be filtered by source interface, domain, destination interface, and policy ID.

In order for information to appear in the **Websites dashboard**, web filtering must be enabled in a policy, with FortiGuard Categories enabled.

The Websites dashboard

Filter Website Domains... | Domains | Categories | now | 5 minutes | 1 hour | 24 hours

Domain	Category	Browsing Time	Threat Weight	Sessions	Bytes (Sent/Received)
nytimes.com	News and Media	2h 3m 9s	0	491	143.70 M
www.bcit.ca	Unknown	12m 45s	0	84	22.90 M
nyt.com	Unknown	13m 24s	0	79	5.20 M
ubc.ca	Education	1h 17m 8s	0	65	3.71 M
moatads.com	Unknown	11m 38s	0	54	2.66 M
sfu.ca	Unknown	7m 16s	0	54	3.46 M
dynamicyield.com	Advertising	12m 1s	0	53	1.07 M
utoronto.ca	Unknown	14s	0	52	1.12 M
ubuntu.com	Reference	21s	0	44	19.59 M
google-analytics.com	Information Technology	1h 37m 38s	0	33	250.86 K
doubleclick.net	Advertising	13m 24s	0	32	467.48 K
cloudfront.net	Unknown	1h 18m 58s	0	31	1.30 M
flashtalking.com	Advertising	2m 32s	0	18	506.25 K
googlesyndication.com	Advertising	13m 24s	0	18	1.54 M
chartbeat.net	Information Technology	2m 21s	0	16	37.93 K
scorecardresearch.com	Business	13m 24s	0	16	215.78 K
krxd.net	Content Servers	10m 1s	0	15	51.83 K
revsci.net	Unknown	11m 38s	0	14	60.04 K
amazonaws.com	Unknown	18m 56s	0	12	622.93 K
fortinet.com	Information Technology	1m 8s	0	12	155.09 K
google.com	Freeware and Software Downloads	15h 26m 5s	0	11	121.19 K

Threats

The **Threats** dashboard lists the top users involved in incidents, as well as information on the top threats to your network. Additional information is provided about the threat, category, threat level, threat weight, and number of incidents.

This dashboard can be filtered by source interface, threat type, threat, destination interface, and policy ID.

In order for information to appear in the **Threats** dashboard, **Threat Weight Tracking** must be used.

The Threats dashboard

Threat	Category	Threat Le...	Threat Weight	Incidents
Failed Connection Attempts	Failed Connection Attempts	Medium	30	3

All Sessions

The **All Sessions** dashboard shows information about all FortiGate traffic. To choose which columns you wish to view, select **Column Settings** and place your desired columns in the right-hand box, in the order that you wish them to appear.

This dashboard can be filtered by source IP, destination IP, application, source device, source interface, destination interface, and policy ID. If you have set a filter in a different dashboard before viewing the **All Sessions** dashboard, that filter will remain until manually cleared.

The All Sessions dashboard

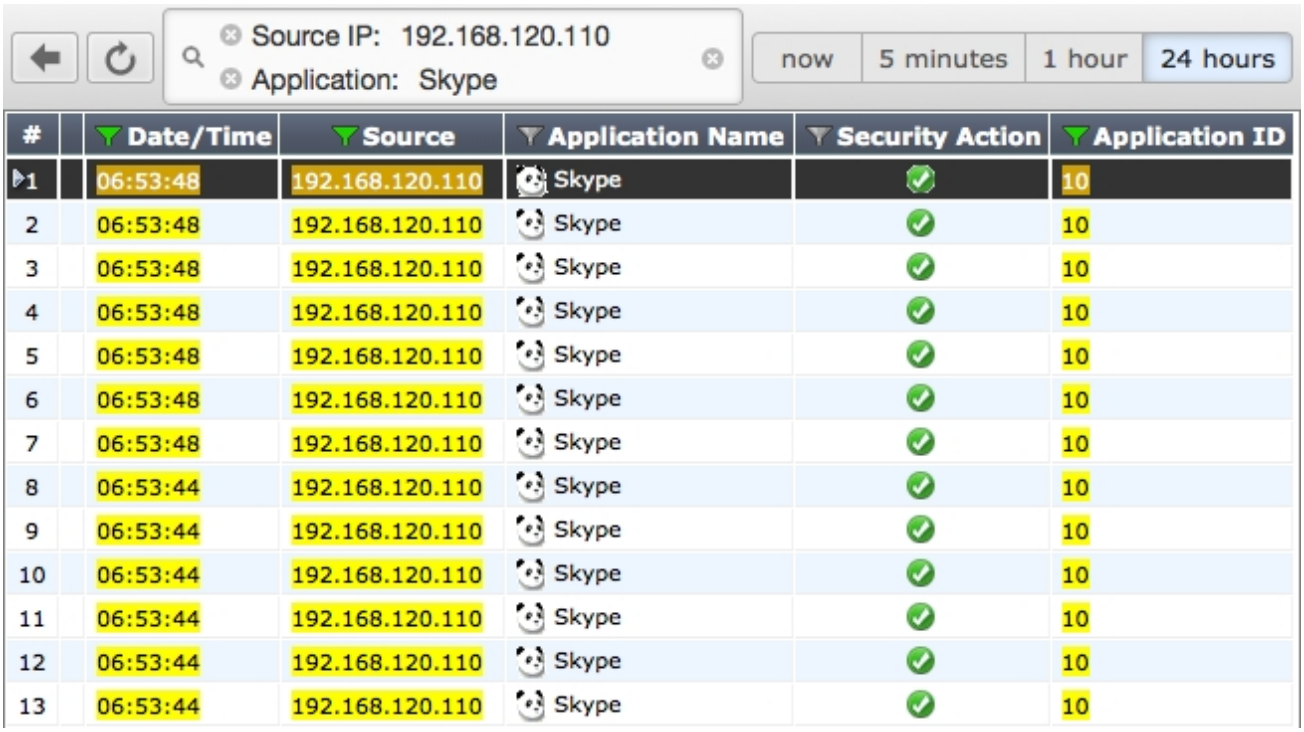
Date/Time	Source	Destination	Application Name	Security Acti...	Threat	Sent / Received
10:49:24	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown			4.11 KB / 11.33 KB
10:49:15	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown		AV EICAR_TEST_FILE	10.65 KB / 237.91 KB
10:44:33	192.168.120.110	38.127.167.7 (lastpass.com)	LastPass			2.02 KB / 8.98 KB
10:44:33	192.168.120.110	108.160.167.148 (d.dropbox.com)	Dropbox_Client.Sync			4.14 KB / 6.59 KB
10:44:26	192.168.120.110	134.170.24.141 (gateway.messenger.live.com)	Skype			10.75 KB / 33.54 KB
10:44:05	192.168.120.110	63.245.217.208 (phx-sync-13-2-8.services.mozilla.com)	SSL			8.66 KB / 4.39 KB

Drilldown Options

In all FortiView dashboards except for the **All Sessions** dashboard, you can view more information about a particular session by right-clicking or double-clicking on the session to display the **Drilldown to details...** option, which opens a summary page that includes further information about applications, sources, destinations, and sessions where applicable.

From this summary page, you can access automatically filtered logs that will show a list of applicable sessions. For example, if you have picked the IP address 192.168.120.110 from the **Sources** dashboard, you can then select **Drilldown to details...** for Skype from the **Applications** column. This will open a log that displays all sessions from 192.168.1.1 that used Skype. From this page, you can select **Drilldown to details...** for any individual session, in order to view the log entry for that session.

Viewing Skype sessions from the Source Address 192.168.120.110



#	Date/Time	Source	Application Name	Security Action	Application ID
1	06:53:48	192.168.120.110	Skype	✓	10
2	06:53:48	192.168.120.110	Skype	✓	10
3	06:53:48	192.168.120.110	Skype	✓	10
4	06:53:48	192.168.120.110	Skype	✓	10
5	06:53:48	192.168.120.110	Skype	✓	10
6	06:53:48	192.168.120.110	Skype	✓	10
7	06:53:48	192.168.120.110	Skype	✓	10
8	06:53:44	192.168.120.110	Skype	✓	10
9	06:53:44	192.168.120.110	Skype	✓	10
10	06:53:44	192.168.120.110	Skype	✓	10
11	06:53:44	192.168.120.110	Skype	✓	10
12	06:53:44	192.168.120.110	Skype	✓	10
13	06:53:44	192.168.120.110	Skype	✓	10

In the **All Sessions** dashboard, filters are also used to narrow down what results are shown. If you are viewing historical traffic in the **All Sessions** dashboard, you can also add an element to a filter by right-clicking the element and selecting **Set Filter**.

Sniffer Traffic Support

Historical traffic logging with the **FortiView** dashboards is supported for sniffer traffic.

FortiExplorer Setup Wizard Improvements

Several improvements have been made to the FortiExplorer Setup Wizard.

Removed Features

Several features have been removed from the FortiGate Setup Wizard:

- Central management configuration
- UTM: AntiSpam setup
- UTM: IPS setup
- Virtual Servers

The WAN Topology options have also been simplified so that the only option is Single Ethernet.

FortiWiFi

Several additional changes have occurred for FortiWiFi units, found in the **LAN + WiFi Settings** section of the wizard:

- The default SSID is now named `fortinetXXXX`, where XXXX is the last 4 digits of the FWF serial number.
- The default SSID is bridged with the internal network.
- The default pre-shared key is different for each FortiWiFi unit.
- A **Show Password** option has been added.

Internet Access

The following changes have been made to the **Internet Access** section of the wizard:

- Selecting **Block Viruses and Malicious Content** enables anti-virus and web filtering
- The MPAA rating system is used for **Parental Controls**

Remote VPN

In the **Remote VPN** section, an option has been added to setup dynamic DNS with FortiGuard. The option is enabled by default.

AntiVirus Inspection Mode

If the flow-based AntiVirus database is not enabled, the setup wizard will change the default profile to proxy-based.

Interfaces List Improvements

Several improvements have been made to the Interfaces List:

- Only interfaces with tunnels or VPNs expand to show more information.
- The Status column shows the number of clients using the interface. Clicking on the number in the status column will direct you to the **DHCP Monitor** or wireless **Client Monitor**, depending on which type of clients are using the interface.
- The protocols listed in the Access column have been assigned color codes. Secure services (HTTPS, SSH) are listed in grey, insecure services (TELNET, HTTP without HTTPS redirect enabled) are listed in red, and all other services are listed in blue.

The Interfaces list

Status	Name	IP/Netmask	Type	Access
	wan1	192.168.0.10 255.255.255.0	Physical	PING FMG-Access AUTO-IPSEC
	wan2	192.168.101.99 255.255.255.0	Physical	PING FMG-Access AUTO-IPSEC
	mesh.root (SSID: fortinet.mesh.root)	0.0.0.0 0.0.0.0	WiFi	
	internal	192.168.1.99 255.255.255.0	Physical	PING HTTPS SSH
	wifi (SSID: NAMAAH)	10.10.80.1 255.255.255.0	WiFi	PING HTTPS FMG-Access

Dragging Objects Between Policies in the Policy List

Objects can now be moved or copied from one policy to another in the policy list. This includes source and destination addresses, services, users, user groups, and security profiles. The default “none” object is also included.

Because of this change, a blank policy can now be created, with the configuration determined by dragging elements from other policies.

Cloning Table Objects

Table objects can now be cloned, allowing an existing object to be copied and given a new name. The object's properties can then be configured by selecting Edit.

Cloning is enabled for both Firewall Objects and Security Profiles.

DHCP-related Improvements in the Web-based Manager

A number of improvements have been made in the web-based manager, relating to DHCP:

- A DHCP Server column has been added to the interface list that shows which interfaces have been enabled as a DHCP server and the assigned IP range.
- The DHCP Client List has been improved by adding device icons and changing the Expires column to show the amount of time left on the DHCP lease.
- New addressing modes have been added to support IPv6 and PPPOE. The option for IPv6 will only appear if it has been enabled in the web-based manager, while PPPOE options only appear if IPv4 addressing is set to PPPOE as well.
- Options have been added to DHCP Monitor, allowing DCCP leases to be revoked and IP reservations to be added or edited.
- Advanced DHCP configuration can now be done through the web-based manager. To enable this feature, the following syntax must be used in the CLI:

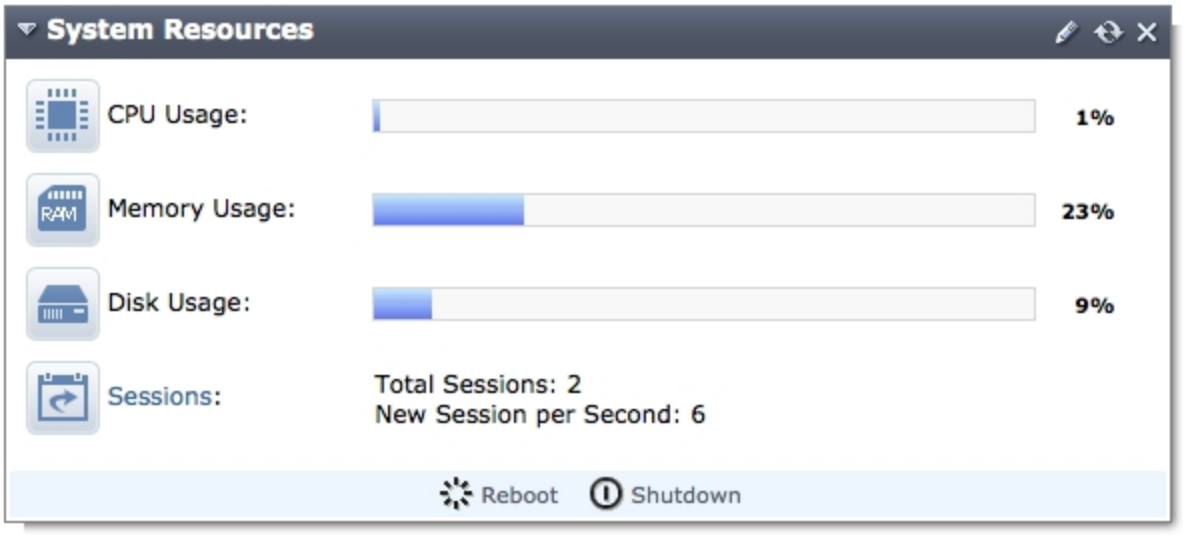
```
config system global
   set gui-dhcp-advanced enable
end
```

After this has been enabled, an **Advanced** menu can be expanded when configuring DCHP on a network interface.

System Resources Widget

The appearance of the **System Resource** widget has been changed to better illustrate the large number of CPU cores. The IPMC sensors information, about temperature, fan, and power supply unit, has also been added to the widget for some FortiGate models.

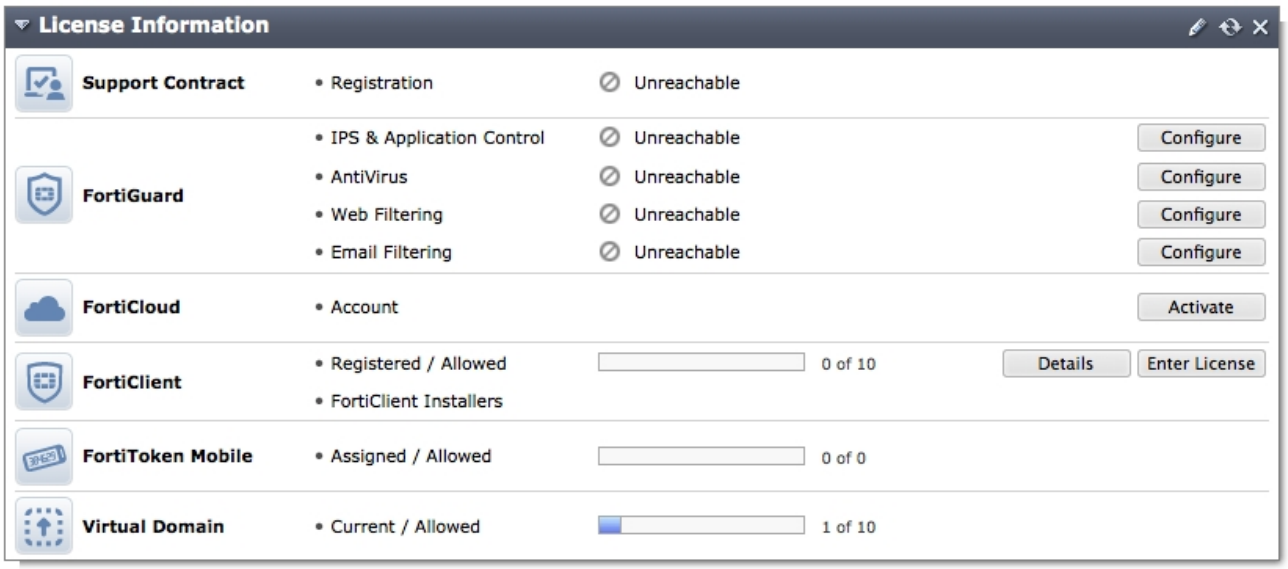
System Resources widget (on a FortiGate-100D)



License Information Widget

The appearance of the **License Information** widget has changed to clearly show the current licenses of your FortiGate. A new option has also been added to extend a license, which allows you to add a new license as soon as you buy it, rather than having to wait for the current license to expire.

License Information widget



USB Modem Widget

The following changes have occurred to the **USB Modem** widget:

- The LOC number has been removed.
- SIM State and SIM card ID fields have been added.
- MEID will be displayed if a CDMA modem is used.
- IMEI will be displayed if a GSM modem is used.

New Feature Settings Preset

A new preset, **UTM**, has been added to the Feature Settings, which are set either using the **Features** widget or by going to **System > Config > Features**. This preset turns on the following features: antivirus, web filtering, application control, and end point control. This preset is the default setting for FortiGate models 200 and below.

The preset formerly known as UTM, which turns on all features, is now called **full UTM**.

Improved Banned User List Page

The banned user list has been improved by the following changes:

- Adding a search function
- Improving sorting through column filters
- Displaying information on the event that caused the user to be quarantined

Replacement Message Improvements

The process of creating replacement message using tags and images has been simplified by the following additions:

- A right-click menu to insert tags/images
- An auto-complete feature for tags (when you begins by entering %%)
- Descriptions for each tag that appear as they are typed
- Image previews when an image tag is used
- An graphics list that allows you to select from predefined images or upload a new image
- Variables for source IP (%%SOURCE_IP%%), destination IP (%%DEST_IP%%), and user name (%%USERNAME%%) can now be added.

Sorting and Filtering Support for the Virtual IP list

In FortiOS, the virtual IP list can be sorted and filtered, allowing for easier management.

Web-based Manager Options for the FortiGate-30D

The FortiGate-30D by default views a different version of the web-based manager than other units, known as `gui-lite`. This mode can be disabled in the CLI, in order to view the standard web-based manager.

Syntax

```
config system global
   set gui-lite disable
end
```

Firewall

New firewall features include:

- Menu Simplification
- Unified Policy Management
- Importing LDAP Users for a Security Policy
- Dynamic VIP According to DNS Translation
- GTP Rate Limiting
- Object UUID Support
- Configuring the Class of Service Bit
- Hairpinning for NAT64 and NAT46
- Maximum Number of Available Virtual IPs Increased

Menu Simplification

Security policies and firewall objects are now found in the same menu, called **Policy & Objects**.

Policies

The menu option for policies, found at **Policy & Objects > Policy,** has been expanded to include the following policy types:

- IPv4
- IPv6
- NAT64
- NAT46
- DoS
- IPv6 DoS
- Multicast
- Local In
- Central NAT Table
- Proxy Options
- SSL Inspection (SSL/SSH Inspection on some FortiGate models)

Objects

The following firewall objects have been grouped together under a single menu, found at **Policy & Objects > Objects**:

- Addresses
- Services
- Schedules
- Traffic Shapers

- Virtual IPs
- IP Pools

Other changes have been made for specific features.

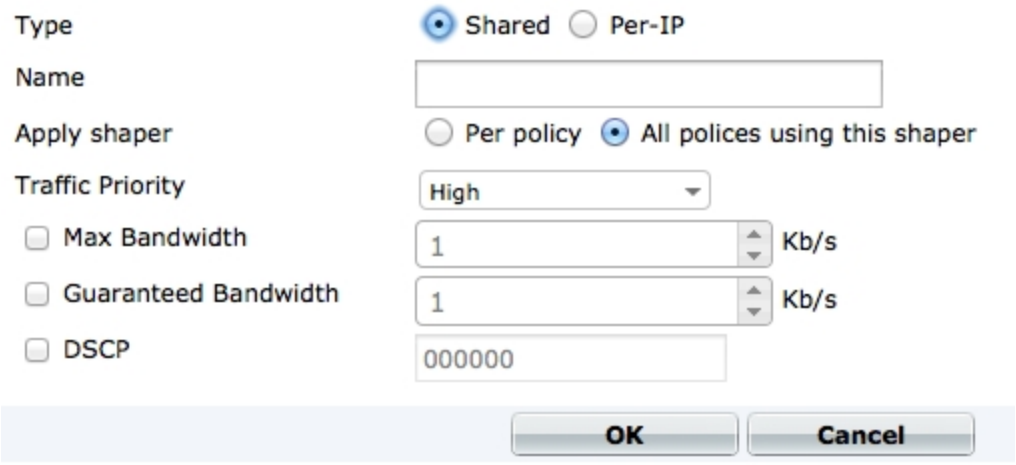
Groups

Object groups can now be made by expanding the arrow beside **Create New** and selecting **Group.**

Traffic Shapers

Shared and Per-IP shapers have been combined into a single page, with a **Type** field added to the creation page.

Traffic shapers creation screen



An additional column, **Type,** has also been added to the traffic shapers table.

Unified Policy Management

The different creation pages in the web-based manager for policy types and subtypes (user-identity, device identity, and VPN) have been merged into a single main policy creation page. New fields have been added for **Source User(s)** and **Source Device Type** that remove the need for multiple authentication rules in a single policy. This allows for greater control and customization of policies, as a combination of these source types can be used in a single policy rather than having to pick one type.

The policy creation page

If both **Source User(s)** and **Source Device Type** are set, then traffic must match both fields in order to be accepted by the policy. Both these fields are optional; only **Source Address** must be set.

For policies that require user or device authentication, there is an implicit fall-through to allow traffic to be checked against other policies if it does not match the authentication requirements. This option cannot be disabled and the CLI command `set fall-through-unauthenticated` has been removed.

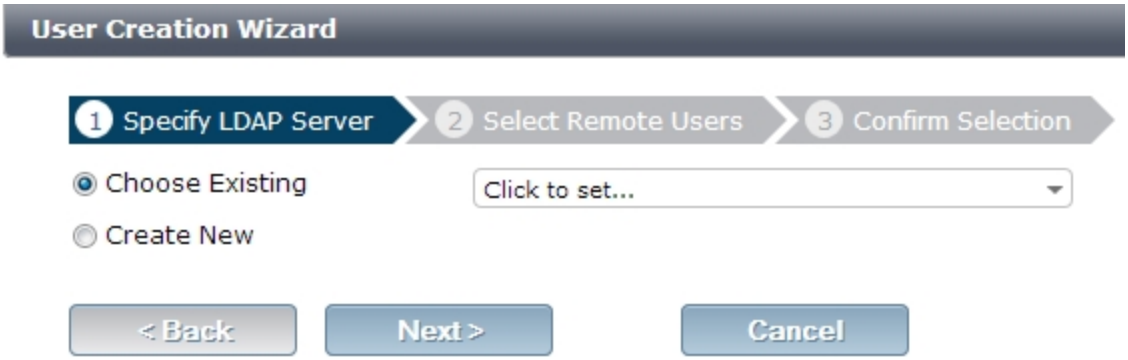
For more information about security policies in FortiOS 5.2, please see the FortiGate Cookbook recipe Creating security policies.

To create a policy for SSL VPNs, an SSL VPN interface is created and used as the source interface. For more information about this interface creation, see SSL VPN Configuration on page 132.

Importing LDAP Users for a Security Policy

The LDAP user importing wizard can now be launched during the creation of a new security policy, by selecting **Import LDAP users** in the dropdown menu when you are adding users to the policy.

The LDAP user importing wizard



Dynamic VIP According to DNS Translation

Dynamic virtual IPs according to DNS translation can now be configured.

When a dynamic virtual IP is used in a policy, the dynamic DNS translation table is installed along with the dynamic NAT translation table into the kernel. All matched DNS responses will be translated and recorded regardless if they hit the policy. When a client request hits the policy, dynamic NAT translation will occur if it matches a record, otherwise the traffic will be blocked.

Syntax

```
config firewall vip
   edit 1
      set type dns-translation
      set extip 192.168.0.1-192.168.0.100
      set extintf dmz
      set dns-mapping-ttl 604800
      set mappedip 3.3.3.0/24 4.0.0.0/24
   end
end
```

GTP Rate Limiting

New methods of GPRS Tunneling Protocol (GTP) rate limiting are available in FortiOS 5.2.

Per-Stream Rate Limiting

FortiOS 5.2 supports per-stream rate limiting of GTP and the ability to apply rate limiting separately for GTPv0 and GTPv1, as well as for GTPv2.

This feature required the addition of the following CLI commands: `message-rate-limit-v0`, `message-rate-limit-v1`, and `message-rate-limit-v2`. The commands `message-rate-limit-v0` and `message-rate-limit-v1` are only visible when `rate-limit-mode` is set to `per-stream`, while message-rate-limit is visible when rate-limit-mode is set to `per-profile`. The command `message-rate-limit-v2` is always visible, since GTPv2 message numbering and naming are different from GTPv0/v1.

The following features have also been added:

- Warning limit support.
- Per-version message rate limiting.
- A log for rate limiting warning called `rate-limited-warning`.

In addition, FortiOS Carrier now indicates the GTP version in rate limiting log messages and writes a rate limiting warning log message when a packet exceeds the rate limiting threshold.

Syntax

```
config firewall gtp
   edit <name>
      set rate-limit-mode {per-profile | per-stream}
      set warning-threshold {0-99}
      config {message-rate-limit-v0 | message-rate-limit-v1 | message-rate-limit-v2}
         set create-pdp-request <rate-limit>
         set delete-pdp-request <rate-limit>
```

```
        set echo-request <rate-limit>
    end
end
```

Per-APN Rate Limiting Profiles

In FortiOS 5.2, GTP rate limiting profiles can be based per-APN, as well as per-IP. To use this feature, the rate limit for each specific APN needs to be configured in the CLI, as there is no default rate limit.

Syntax

```
config firewall gtp profile
   set rate-limit-mode per-apn
   config per-apn-shaper
      edit <ID>
         set apn <string>
         set version <version>
         set rate-limit <rate-limit>
      end
end
```

Object UUID Support

UUID is only supported on large-partition platforms (>=128M).

A Universally Unique Identified (UUID) attribute has been added to some firewall objects, including virtual IPs and virtual IP groups for IPv4, IPv6, NAT46, and NAT64, so that the logs can record these UUID to be used by a FortiManager or FortiAnalyzer unit.

The UUID of an object can either be generated automatically or assigned through the CLI. To view the UUID for these objects in a FortiGate unit's logs, `log-uuid` must be set to `extended mode`, rather than `policy-only`, which only shows the policy UUID in a traffic log.

Syntax

```
config sys global
   set log-uuid {disable | policy-only | extended}
end

config firewall {policy | policy6 | policy46 | policy64 | address| addres6 | addgrp |
    addgrp6}
   edit <1>
      set uuid <8289ef80-f879-51e2-20dd-fa62c5c51f44>
   end
end
```

Configuring the Class of Service Bit

FortiGate units can now configure the value of the Class of Service (CoS) bit, also called Priority Code Point (PCP).

The value of CoS in forward direction (fwd) and reverse direction (rev) is set in the policy/policy6 table using the CLI. The value can be set either as 255, to allow passthrough, or given a priority between 0 and 7.

Syntax

```
config firewall {policy | policy6}
   set vlan-cos-fwd <int>
   set vlan-cos-rev <int>
end
```

Hairpinning for NAT64 and NAT46

In FortiOS 5.2, NAT64 and NAT46 support hairpinning between hosts that are located in the same network behind a single external IP address. Hairpinning allows endpoints on the internal network to communicate using external IP addresses and ports.

In order to allow hairpinning, `set permit-any-host` must be enabled in the NAT64 or NAT46 firewall policy.

Maximum Number of Available Virtual IPs Increased

The maximum limit of available virtual IPs has been increased on 1U FortiGate models (FortiGate-100 to 800 series) to 16,000 and on 2U FortiGate models (FortiGate-1000 to 3810 series) to 32,000.

Security Profiles

New security profiles features include:

- Menu and Options Simplification
- SSL Inspection
- Web Filtering
- Application Control
- Flow-based Antivirus
- Intrusion Protection System (IPS)
- Vulnerability Scanning Visibility
- Removed IM Proxy Options from CLI
- Client Reputation

Menu and Options Simplification

The menus and options for security profiles have changed in several ways. The basic profile/sensor/settings options have been left in the menu for each feature, while extra tables are now located in the **Advanced** menu. Other changes have been made for specific features.

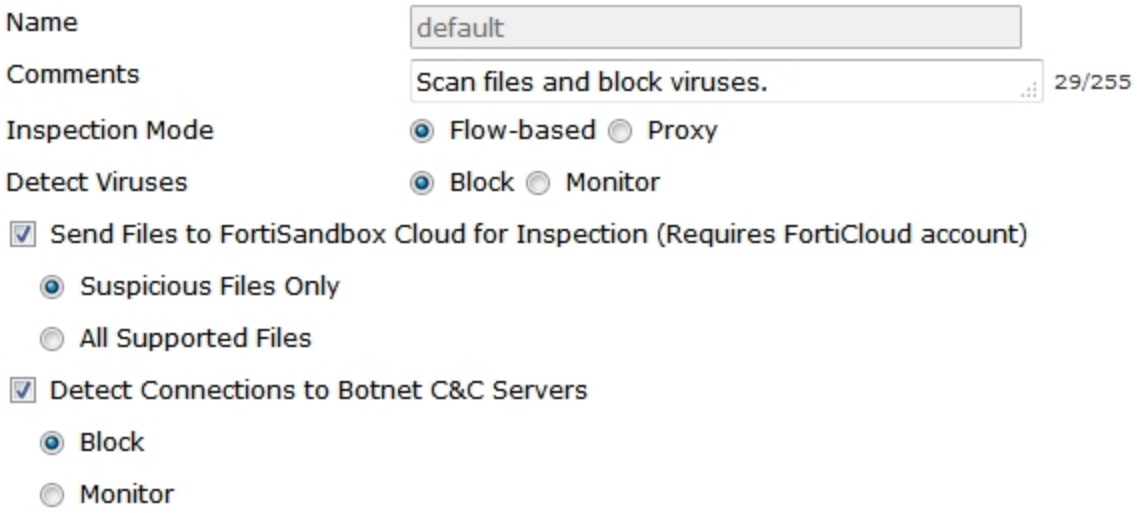
AntiVirus

Several changes have been made for the configuration options in AntiVirus profiles, as visible options change depending on whether **Inspection Mode** is set to **Flow-based** or **Proxy**.

Flow-based Profile Options

If flow-based inspection is used for AntiVirus, you can configure whether to send files to **FortiSandbox Cloud** for inspection as well as the actions to be taken for detected viruses, and for connections to **Botnet C&C** servers. You can send suspicous files or all supported files to FortiSandbox cloud. Detect Viruses and connections to Botnet C&C Servers can be set to either Block or Monitor.

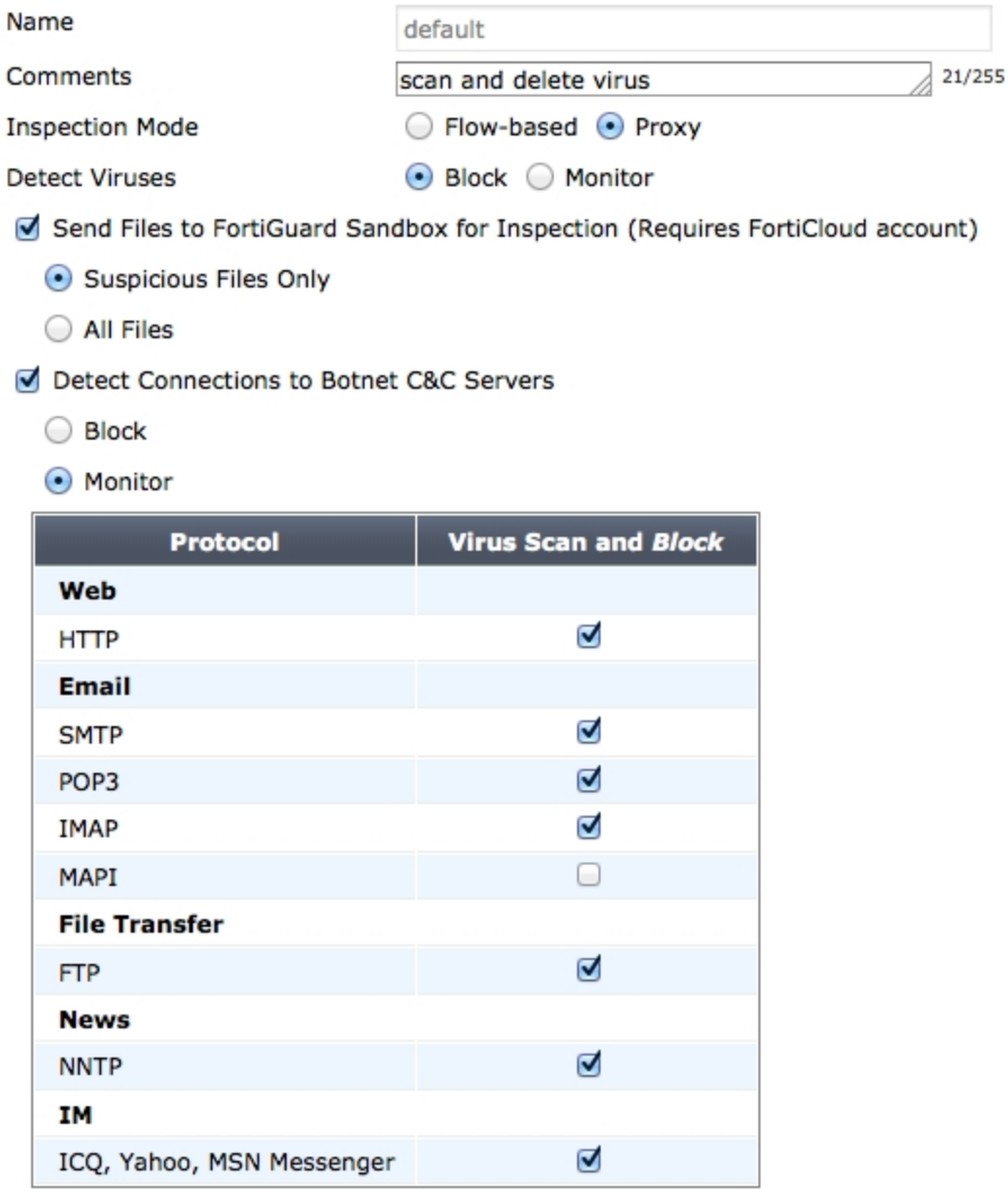
Flow-based options for AntiVirus



Proxy Options

If proxy inspection is used for AntiVirus, the addition **Block** or **Monitor** options are available for both detected viruses and Botnet C&C servers. The previous options for using FortiSandbox and protocol selection are also available.

Proxy options for AntiVirus

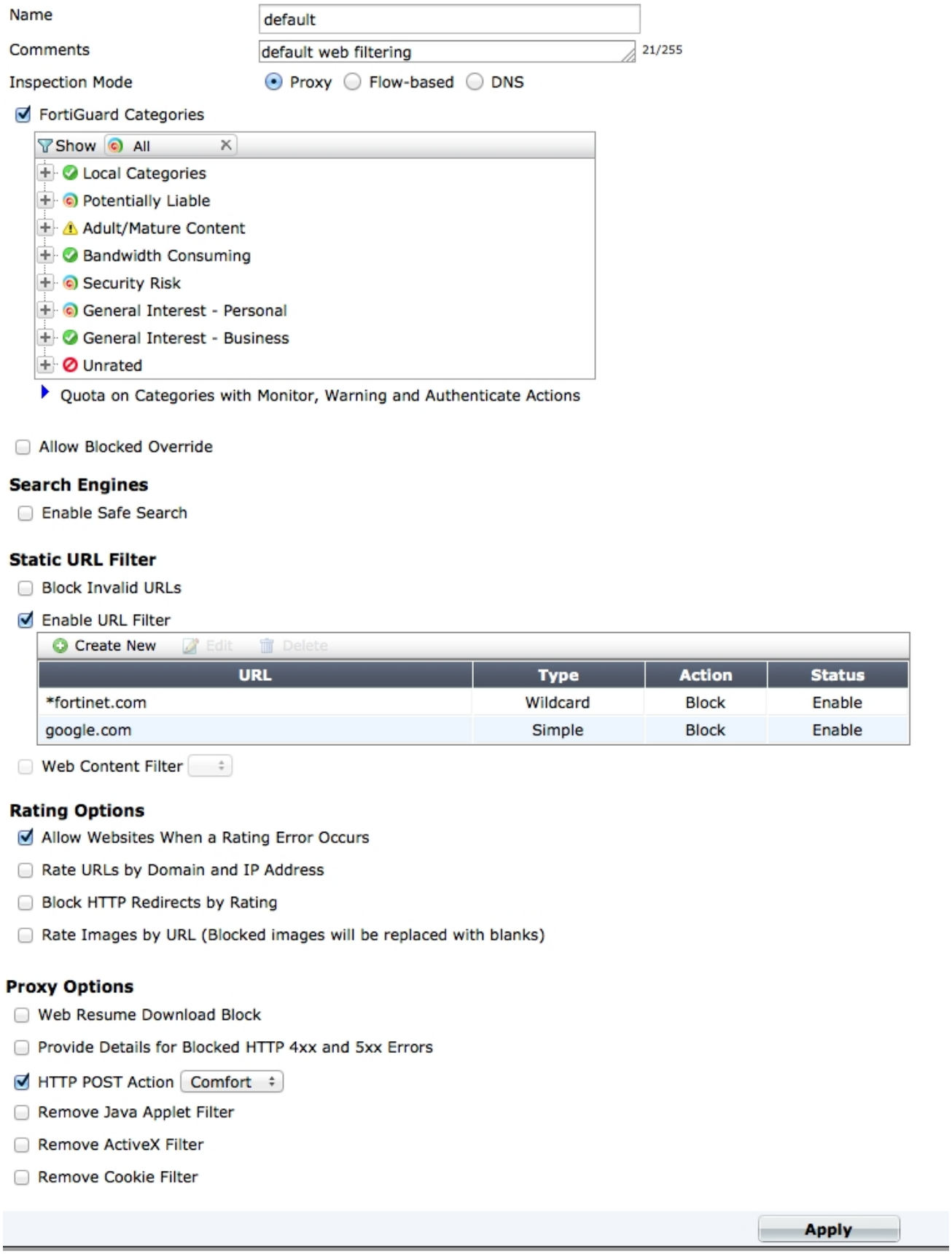


Protocol	Virus Scan and *Block*
Web	
HTTP	☑
Email	
SMTP	☑
POP3	☑
IMAP	☑
MAPI	☐
File Transfer	
FTP	☑
News	
NNTP	☑
IM	
ICQ, Yahoo, MSN Messenger	☑

Web Filter

The web filter profile page has been expanded to contain settings for **FortiGuard Categories**, **Search Engines**, **URL Filters**, **Ratings Options**, and **Proxy Options**.

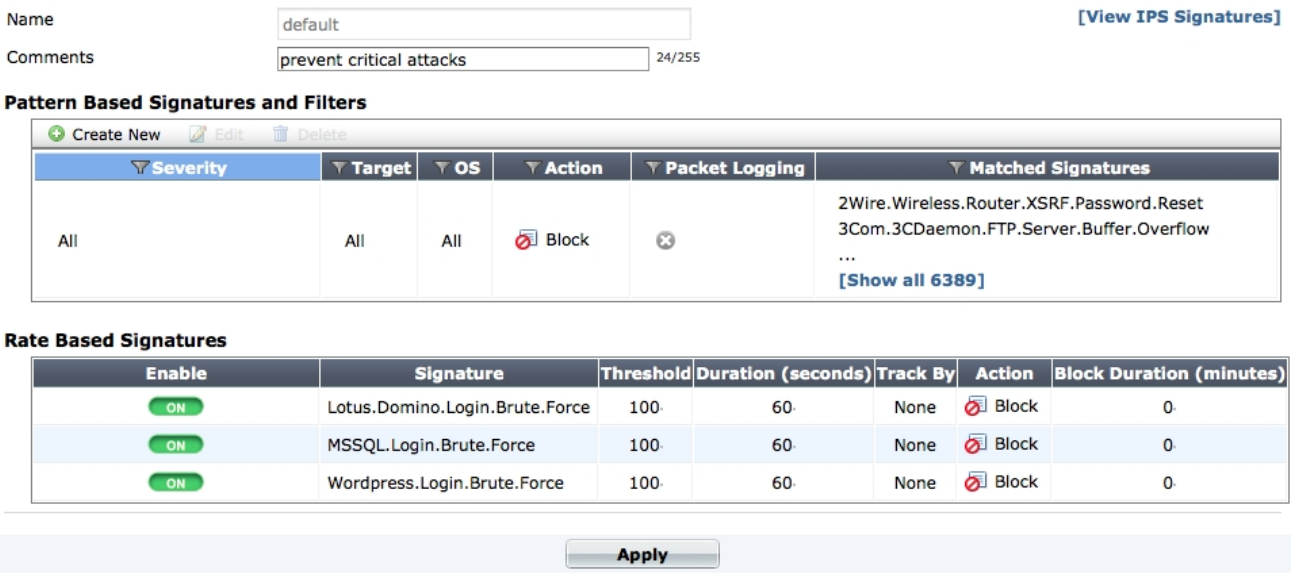
The web filter profile page


Name
default
Comments
default web filtering
21/255
Inspection Mode
Proxy
Flow-based
DNS
FortiGuard Categories
Show
All
Local Categories
Potentially Liable
Adult/Mature Content
Bandwidth Consuming
Security Risk
General Interest - Personal
General Interest - Business
Unrated
Quota on Categories with Monitor, Warning and Authenticate Actions
Allow Blocked Override
Search Engines
Enable Safe Search
Static URL Filter
Block Invalid URLs
Enable URL Filter
Create New
Edit
Delete
URL
Type
Action
Status
*fortinet.com
Wildcard
Block
Enable
google.com
Simple
Block
Enable
Web Content Filter
Rating Options
Allow Websites When a Rating Error Occurs
Rate URLs by Domain and IP Address
Block HTTP Redirects by Rating
Rate Images by URL (Blocked images will be replaced with blanks)
Proxy Options
Web Resume Download Block
Provide Details for Blocked HTTP 4xx and 5xx Errors
HTTP POST Action
Comfort
Remove Java Applet Filter
Remove ActiveX Filter
Remove Cookie Filter
Apply

Intrusion Protection

The IPS sensor page now contains options for **Pattern Based Signatures and Filters** and **Rate Based Signatures**. The full list of IPS Signatures can be accessed from the sensor page by selecting **View IPS Signatures**.

The IPS sensor page

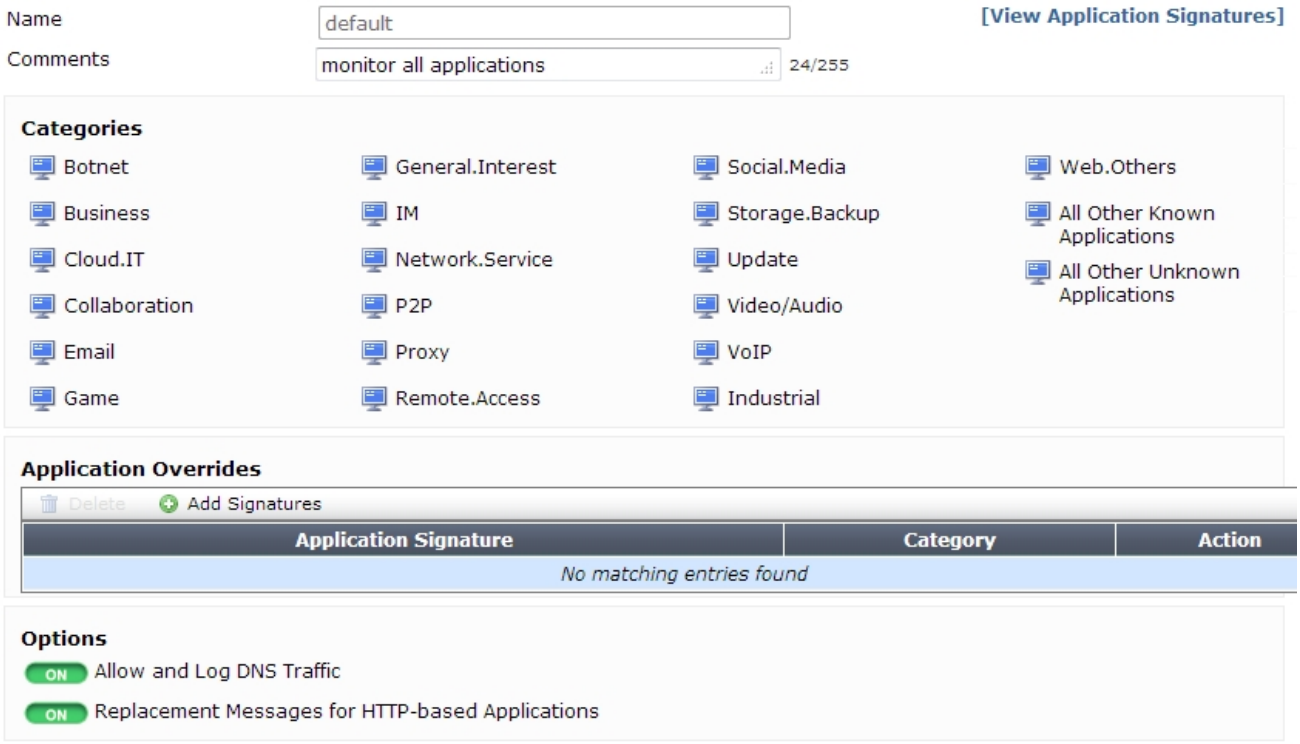


Application Control

The following changes have been made to improve usability in the web-based manager:

- A new category list has been made that appears on the sensor page, found by going to **Security Profiles > Application Control**. When you click on a category, a drop down menu appears, allowing the action for that category to be changed. You can also select to view all the application control signatures for that category.
- Application signatures can be viewed by selecting **View Application Signatures**.
- **Application Overrides** allow you to change the action taken for specific signatures/applications.
- The application filter sorting criteria popularity, technology, and risk have been removed.

The application control sensor page



Advanced Options

A new advanced menu has been added that contains the following features:

- Web rating overrides
- Web profile overrides
- DLP fingerprinting

Web Rating Overrides can also now be used to edit or delete custom website categories.

SSL Inspection

There have been several changes to how SSL Inspection is handled on a FortiGate unit.

Automatic Inspection When Security Profiles are Used

If any security profile is used in a security policy, SSL inspection will automatically be enabled, at which point an SSL mode must be selected (see below for more details).

HTTPS Scanning Without Deep Inspection

The following changes have been made in order to allow HTTPS traffic to be scanned without enabling deep inspection:

- There are now two modes for SSL inspection: certificate inspection (`certificate-inspection` in the CLI), which only inspects the SSL handshake, and `deep inspection (deep-inspection` in the CLI), which enables full deep inspection of SSL traffic (this was previously the default mode for SSL inspection).
- The CLI command `https-url-scan` has been removed.
- `deep-inspection-options` has been renamed `ssl-ssh-profile`.
- The SSL `inspect-all` option and the `https status` option now have three states: `disable`, `certificate-inspection`, and `deep-inspection`. The status option for the other protocols now use `deep-inspection` instead of `enabled`.

When a new policy or profile group is created, the SSL inspection profile `certificate-inspection` is automatically added.

SSL/Deep Inspection Exemptions

The options for configuring exemptions to SSL/Deep Inspection is now configured as part of the deep inspection options, rather than FortiGuard web filtering. Exemptions can be added to SSL inspection by going to **Policy & Objects > Policy > SSL Inspection** or through the CLI.

Certain applications, such as iTunes and Dropbox, require a specific certificate to be used, rather than using the use the system's certifciate store. Because of this, the default deep inspection profile, `deep-inspection`, has exemptions configured for these applications by default in FortiOS 5.2.

Syntax

```
config firewall ssl-ssh-profile
   edit <name>
      config ssl-exempt
         edit <id>
            set type {fortiguard-category | address | address6}
            set category <id>
            set address <string>
         end
   end
```

Generating Unique CA and Server Certificates

A FortiGate unit will now generate default SSL inspection CA and server certificates that are unique to that unit the first time the certificates are required. Previously, FortiGate units all have the same default CA and server certificates.

There are some exceptions: for example, in a HA cluster all FortiGate units need the same CA and server certificates. The certificates can also be changed as required for load balancing and other configurations.

Existing customers will not be affected by this change, as FortiOS 5.2 will not change the current defaults on upgrade.

You can use the CLI commands below to generate new certificates that will be unique to your FortiGate unit.

The following command re-generates the default SSL inspection CA certificate:

```
execute vpn certificate local generate default-ssl-ca
```

The following command re-generates the default SSL inspection server certificate:

```
execute vpn certificate local generate default-ssl-serv-key
```

Server Certificates

In FortiOS 5.2, two methods are available to support server certificates and allow inbound traffic to be inspected: **Multiple Clients Connecting to Multiple Servers** (`re-sign` in the CLI) or **Protecting SSL Server** (`replace` in the CLI).

The default setting for SSL Inspection is **Multiple Clients Connecting to Multiple Servers.** This setting can be changed by going to **Policy & Objects > Policy > SSL Inspection** or through the CLI.

Syntax

- Uploading a new server certificate:

```
config firewall ssl-ssh-profile
   edit <name>
      set server-cert-mode replace
      set server-cert <certificate>
   end
end
```

- Re-signing the server certificate:

```
config firewall ssl-ssh-profile
   edit <name>
      set server-cert-mode re-sign
      set caname <name>
      set certname <name>
   end
end
```

Web Filtering

There have been several changes made to web filtering in FortiOS 5.2.

HTTPS for Warnings and Authentication

HTTPS protocol can now be used when sending web filtering warnings or requiring a user to authenticate, including authentication for web filter overrides.

Syntax

```
config webfilter fortiguard
   set ovrd-auth-https enable
   set warn-auth-https enable
end
```

Modifying HTTP Request Headers

In FortiOS 5.2, you can add, modify, and remove header fields in HTTP request when scanning web traffic in proxy-mode. If a header field exists when your FortiGate receives the request, its content will be modified based on the configurations in the URL filter.

Syntax

```
config web-proxy profile
```

```
edit <name>
   config headers
      edit <ID>
         set name <name>
         set content <string>
      end
end
```

Restrict Google Access to Corporate Accounts

A new option has to web filtering to restrict Google access to specific domains. This allows you to block access to some Google accounts and services while allowing access to corporate Google accounts.

To use this option, go to **Security Profiles > Web Filter** and select **Restrict Google Account Usage to Specific Domains** under **Proxy Options**. You can then add the appropriate Google domains that will be allowed.

After the web filter profile has been created, this feature is applied differently in the case of transparent proxy vs. explicit proxy. For transparent proxy, the web filter profile is added to a security policy. For explicit proxy, the web filter profile must be added to an explicit proxy profile.

This feature can also be configured using the CLI, where use of the Modifying HTTP Request Headers feature (see above) is required. In the following example, access to Personal Gmail accounts is blocked while access to Google Business Mail is allowed.

Syntax

1. The web-proxy profile is configured to with a modified header:

```
config web-proxy profile
   edit "restrict-google-accounts-1"
      config headers
         edit 1
            set name "X-GoogApps-Allowed-Domains"
            set content "example.com"
         end
   end
```

2. A URL filter is configured to use the web-proxy profile:

```
config webfilter urlfilter
   edit 1
      set name "GMAIL_TEST"
      config entries
         edit 1
            set url "*.google.com"
            set type wildcard
            set action allow
            set web-proxy-profile "restrict-google-accounts-1"
         end
   end
```

3. A webfilter profile is configured that uses the URL filter:

```
config webfilter profile
   edit "GMAIL_TEST"
      ......
      config web
         set urlfilter-table 1
```

```
      end
      config ftgd-wf
         ......
      end
end
```

4. **Transparent proxy -** the webfilter profile is applied to a security policy:

```
config firewall policy
   edit 1
      set srcintf "LAN"
      set dstintf "WAN"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set webfilter-profile "GMAIL_TEST"
      set profile-protocol-options "default"
      set ssl-ssh-profile "deep-inspection"
      set nat enable
   end
end
```

5. **Explicit proxy -** the web-proxy policy and the web filer profile are applied to an explicit proxy policy:

```
config firewall explicit-proxy-policy
   edit 1
      set proxy web
      set dstintf "WAN"
      set srcaddr "all"
      set dstaddr "all"
      set service "webproxy"
      set action accept
      set schedule "always"
      set webproxy-profile "restrict-google-accounts-1"
      set utm-status enable
      set webfilter-profile "GMAIL_TEST"
      set profile-protocol-options "default"
      set ssl-ssh-profile "deep-inspection"
   end
end
```

Referer Added to URL Filtering

You can now add a referer to URL filters. If a referer is specified, the host name in the referer field of the HTTP require will be compared for any entry that contains the matching URL. If the referer matches, then the specified action will be performed by proxy.

The referer can also be set in the web-based manager, but only if advanced web filter features has been enabled using the following command:

```
config system global
   set gui-webfilter-advanced enable
end
```

After this command is used, a new column will be created in **Security Profiles > Web Filter > Static URL Filter** to set the referer.

The command `set referrer-host` has been added to the CLI. The CLI has also changed so that URL filters are now identified by their IDs, and the URL values can be set under each entry.

Syntax

```
config webfilter urlfilter
   edit <ID>
      config entries
         edit 1
            set url <url>
            set referrer-host <url>
            set type {simple | regex | wildcard}
            set action {block | allow | monitor | exempt}
            set status {enable | disable}
         end
   end
```

FortiGuard Rating Checks for Images, JavaScript, CSS, and CRL

Web filter profiles that use FortiGuard rating checks can now be configured to rate images, JavaScript, CSS, and CRL.

Syntax

```
config webfilter profile
   edit <name>
      config ftgd-wf
         set rate-javascript-urls enable
         set rate-css-urls enable
         set rate-crl-urls enable
         set rate-image-urls enable
      end
end
```

Additional Replacement Message Variables

Along with the variables for source IP (%%SOURCE_IP%%), destination IP (%%DEST_IP%%), and user name (%%USERNAME%%) that have been added for all replacement messages, the following variables can now be added to replacement messages for web filtering:

- Group name (%%GROUPNAME%%)
- Policy UUID (%%POLICY_UUID%%)
- FortiGate Hostname (%%FGT_HOSTNAME%%)

New Daemon for Overrides and Warnings

The new daemon `ovrd` is used in FortiOS 5.2 to handle user-level webfilter overrides and warnings.

Application Control

There have been several changes made to application control.

Deep Inspection for Cloud Applications

Deep inspection allows the following information to be examined and logged for cloud applications:

Information about user logins and file transfers for cloud applications.

Video names will be shown in the **Application Details** column for video streaming applications such as Youtube and Vimeo.

The following new fields have been added to both the application control log and to traffic logs: cloud user, cloud action, file name, and file size.

To enable this feature, turn on **Deep Inspection of Cloud Applications** in an application control profile. It can also be enabled using the CLI.

Syntax

```
config application list
   edit <name>
      set deep-app-inspection enable
   end
end
```

Using the CLI, you can specify a global timeout for the deep application control database. Any database entries that exceed the timeout will be deleted. A global size threshold on the number of entries in the deep application control database can also be set.

When the total number of entries exceeds this threshold, the internal timeout value will be reduced to accelerate entry retiring. Both values are set to 0 (unlimited) by default.

Syntax

```
config ips global
   set deep-app-insp-timeout <integer>
   set deep-app-insp-db-limit <integer>
end
```

A new option, `--deep_ctrl`, has also been added to the syntax for IPS/application control signatures.

Several new CLI commands have also been added for diagnose and debugging:

- `diagnose ips dac info`
- `diagnose ips dac clear`
- `diagnose ips debug enable dac`

Traffic Shaping Settings

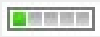
Traffic shaping settings can be applied to categories of applications that are part of the application control sensor.

To apply settings, select a category and set it to **Traffic Shaping.** The **Traffic Shaping Settings** options will appear, allowing you to select the settings for forward and reverse traffic shaping. These settings will be applied to all categories set to **Traffic Shaping** in your application control sensor.

5-Point-Risk Rating

A new rating system will be used for all pages related to application control, including the application list, the application filters list, traffic logs, the **FortiView Applications** dashboard, and the **FortiView All Sessions** dashboard. Risk levels are indicated in the various tables and logs by using a series of icons.

The rating system is as follows:

Icon	Risk Level	Description	Example
	Critical	Applications that are used to conceal activity to evade detection	Tor, SpyBoss
	High	Applications that can cause data leakage, or prone to vulnerabilities or downloading malware	Remote Desktop, File Sharing, P2P
	Medium	Applications that can be misused	VoiP, Instant Messaging, File Storage, WebEx, Gmail
	Elevated	Applications are used for personal communications or can lower productivity	Gaming, Facebook, Youtube
	**Low**	Business Related Applications or other harmless applications	Windows Updates

Replacement Message

A replacement message has been added that will appear when an application has been blocked.

This replacement message can be enabled in the CLI.

Syntax

```
config application list
   edit <name>
      set app-replacemsg {enable | disable}
   end
end
```

Support for SPDY Protocol

The SPDY protocol, and its required SSL/TLS component, is now recognized within application control profiles. It is counted as part of application traffic for Google and other sources that use the protocol.

Support for Non-HTTP WAN Optimization and Explicit Proxy Traffic

Application control is now supported for both non-HTTP WAN optimization traffic and explicit proxy traffic.

Flow-based Antivirus

In FortiOS 5.2, flow-based AntiVirus has been improved to have the same enhanced performance as flow-based antivirus scanning in FortiOS 5.0 while providing the same accuracy and many of the extended features of proxy-based antivirus.

Flow-based AntiVirus now allows data to accumulate until it detect the end of a file. When the end is reached, traffic is paused and data is sent asynchronously for analysis. When the results are received, the traffic is either allowed to resume or the connection is reset.

Because of this change, the default AntiVirus profile on a FortiGate uses flow-based inspection. Flow-based inspection can also utilize the extended AntiVirus database. Detecting and reporting only occurs when AntiVirus is enabled in the security policy.

Flow-based AntiVirus is also supported for sniffer policies.

Intrusion Protection System (IPS)

There have been several changes made to intrusion protection system (IPS).

Adjusting Rate Based Signatures

Setting for rate based IPS signatures can now be edited in the web-based manager as part of an IPS sensor. In each sensor, you can enable a selected list of rate based signatures and adjust threshold, duration, track by setting, action, and block duration.

Rate Based Signatures list

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
ON	Lotus.Domino.Login.Brute.Force	100	60	None	Block	0
ON	MSSQL.Login.Brute.Force	100	60	None	Block	0
ON	Wordpress.Login.Brute.Force	100	60	None	Block	0

Extensible Meta Data

Extensible meta data allow you to specify custom options in IPS signatures that are delivered to your FortiGate without interpretation, in order to make signatures easier to find and understand for the FortiGate administrator. Four types of meta data options are supported: integers, bitmaps, enumerables, and strings.

Example

In this example, a set of meta data is declared and then used to create IPS signatures.

The meta data is declared:

```
F-META2( --name points; --index 12; --type integer; )
F-META2( --name flags; --index 34; --type bitmap; --value foo:1; --value bar:2; --value
    baz:4; )
F-META2( --name dr_seuss; --index 56; --type enum; --value "One Fish":1; --value "Two
    Fish":2; --value "Red Fish":3; --value "Blue Fish":4; )
F-META2( --name secret; --index 78; --type string; )
```

The meta data is used:

```
F-SBID( --points 42; ... )
F-SBID( --flags foo; --flags baz; ... )
F-SBID( --dr_seuss "One Fish"; ... )
F-SBID( --secret "Abracadabra"; ... )
```

Extended Database

In FortiOS 5.2, the IPS extended database is enabled by default for all FortiGate models that have multiple CP8.

Support for Non-HTTP WAN Optimization and Explicit Proxy Traffic

IPS is now supported for both non-HTTP WAN optimization traffic and explicit proxy traffic.

Vulnerability Scanning Visibility

The options to configure vulnerability scanning either in the web-based manager or the CLI are also only available in NAT/Route mode.

Vulnerability scanning options in the web-based manager are now hidden by default. To enable vulnerability scanning, go to **System > Config > Features**, select **Show More**, turn on **Vulnerability Scan**, and select **Apply**.

Vulnerability scanning is also hidden by default for FortiClient profiles until being enabled in the CLI. To enable scanning, enter the following commands:

```
config endpoint-control profile
   edit <profile-name>
      config forticlient-winmac-settings
         set forticlient-vuln-scan {enable | disable}
         set forticlient-vuln-scan-schedule {daily | weekly | monthly}
         set forticlient-vuln-scan-on-registration {enable | disable}
         set forticlient-ui-options {av | wf | af | vpn | vs}
      end
end
```

Removed IM Proxy Options from the CLI

The proxy options related to instant messaging (IM) functions and attributes have been removed from the CLI in FortiOS 5.2. This includes the following commands:

- `config imp2p`
- `get imp2p`
- The DLP sensor options for AIM, ICQ, MSN, and Yahoo protocols.
- The AntiVirus profile option `config im`.
- The AntiVirus quarantine options for IM.
- The Application Control profile options for IM.
- The firewall profile protocol options for IM.

Client Reputation

The 5.0 feature client reputation has been renamed Threat Weight in FortiOS 5.2 and has been moved from Security Profiles to **Log & Report > Log Config > Threat Weight**. It can now be configured in the CLI using the command `config log threat-weight`.

IPsec VPN

New IPsec VPN features include:

- VPN Creation Wizard
- Internet Key Exchange (IKE)
- Dynamic IPsec Route Control
- Default Lifetimes and Proposal Values
- Prioritizing DH Group Configuration
- IPv6 Support for IPsec Phase 2
- IPsec VPN Support with the FortiController-5103B

VPN Creation Wizard

Several improvements have been made to the **VPN Creation Wizard.**

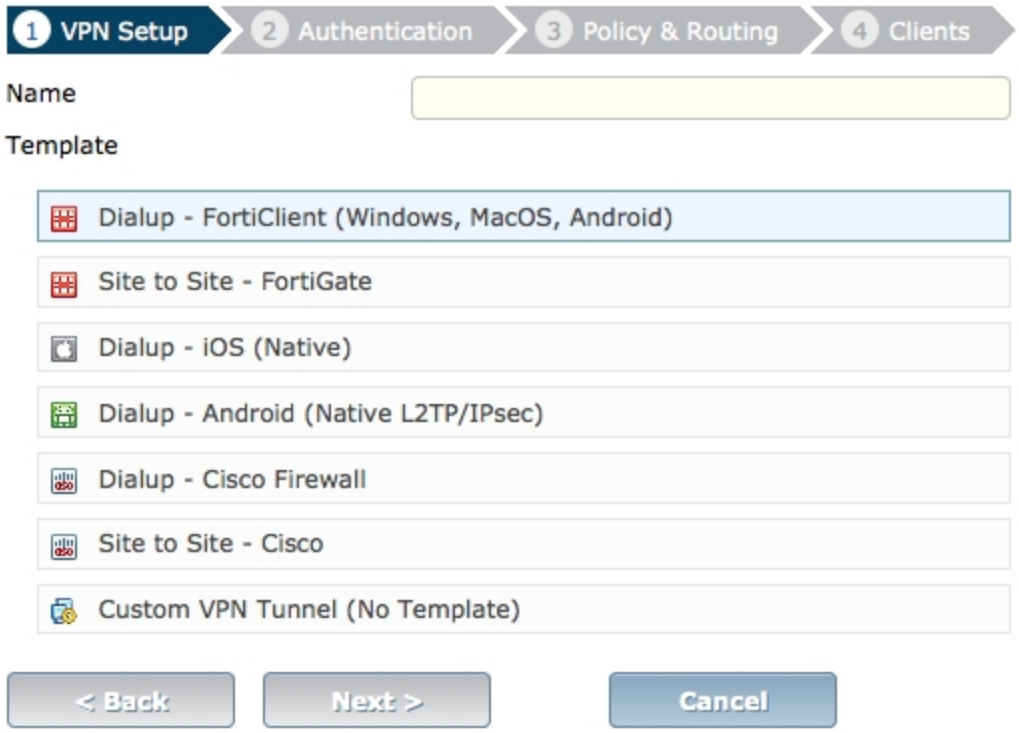
New Menu

The Wizard can now be found by going to **VPN > IPsec > Wizard.**

Expanded VPN Options

The number of VPN options available in the Wizard has increased to allows you to easily create VPN tunnels for a greater variety of scenarios.

Expanded VPN Options for the VPN Creation Wizard



For more information about using the VPN Wizard, see The FortiGate Cookbook recipe IPsec VPN for iOS devices.

Tunnel Templates

Several tunnel templates have been added to the Wizard that cover a variety of different types of IPsec VPNs. A list of these templates appears on the first page of the Wizard, which is found by going to **VPN > IPsec > Tunnels**.

To view more information about a template, highlight the template and select **View.**

Tunnel Templates list

Template	Description
Dialup - FortiClient (Windows, MacOS, Android)	On-demand tunnel for users using the FortiClient software.
Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec client.
Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client.
Dialup - Cisco Firewall	On-demand tunnel for users using the Cisco IPsec client.
Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.

Internet Key Exchange (IKE)

There have been several changes in FortiOS 5.2 made concerning Internet Key Exchange (IKE) protocol.

Multiple Interfaces

An IPsec policy can now contain multiple source and destination interfaces. This feature is supported for combinations of IPsec interfaces, physical interfaces, and zones (including those with a combination of physical and IPsec interfaces).

It is not supported for SSL VPN interfaces.

Mode-Configuration

When IKE Mode-Configuration is enabled, multiple server IPs can be defined in IPsec Phase 1. This mode also allows IP information to be sent the client if attribute 28681 is requested.

Mode-Configuration is configured through the CLI. An example of a complete configuration is shown below:

```
config vpn ipsec phase1-interface
   edit "vpn-p1"
      set type dynamic
      set interface "wan1"
      set xauthtype auto
      set mode aggressive
      set mode-cfg enable
      set proposal 3des-sha1 aes128-sha1
      set dpd disable
      set dhgrp 2
      set xauthexpire on-rekey
      set authusrgrp "FG-Group1"
      set ipv4-start-ip 10.10.10.10
      set ipv4-end-ip 10.10.10.20
      set ipv4-dns-server1 1.1.1.1
      set ipv4-dns-server2 2.2.2.2
      set ipv4-dns-server3 3.3.3.3
      set ipv4-wins-server1 4.4.4.4
      set ipv4-wins-server2 5.5.5.5
      set domain "fgt1c-domain"
      set banner "fgt111C-banner"
      set backup-gateway "100.100.100.1" "100.100.100.2" "host1.com" "host2"
   end
end
```

Certificates Groups

IKE certificate groups consisting of up to four RSA certificates can now be used in IKE phase 1. Since CA and local certificates are global, the IKE daemon loads them once for all VDOMs and indexes them into trees based on subject and public key hash (for CA certificates), or certificate name (for local certificates). Certificates are linked together based on the issuer, and certificate chains are built by traversing these links. This reduces the need to keep multiple copies of certificates that could exist in multiple chains.

IKE certificate groups can be configured through the CLI.

Configuring the IKE local ID

```
config vpn certificate local
   edit <name>
      set ike-localid <string>
      set ike-localid-type {asn1dn | fqdn}
   end
end
```

Adding certificates to the group

```
config vpn ipsec {phase1 | phase1-interface}
   edit <name>
      set rsa-certificate <name>
   end
end
```

Authentication Methods

Three new authentication methods have been implemented for IKE: ECDSA-256, ECDSA-384, ECDSA-521.

In order to support these three methods, the following changes have been made to the CLI:

1. `rsa-signature` has been renamed to `signature` for both policy-based and interface-based IPsec VPN.
2. `rsa-certificate` has been renamed to `certificate` for both policy-based and interface-based IPsec VPN.

Inheriting Groups from the Security Policy

IPsec VPNs can now be configured to authenticate users again the group(s) specified in a policy that refers to the VPN's phase 1. To use this feature, do the following:

1. Go to **VPN > IPsec > Tunnels** and edit a tunnel.
2. Set **XAUTH Type** to **Auto Server**.
3. Set **User Group** to **Inherit Groups from Policy**.

This feature can be used for both interface-based and policy-based IPsec VPN phase 1s.

Syntax

```
config vpn ipsec {phase1 | phase1-interface}
   edit <name>
      set xauthtype auto
   end
end
```

Assigning Client IP Addresses Using the DHCP Proxy

IKE can now use the system DHCP proxy to assign client IP addresses.

To use this feature, the DHCP proxy must be enabled and a IP set. Up to 8 addresses can be selected for either IPv4 or IPv6. After the DHCP proxy has been configured, the `assign-ip-from` command is used to select assign IP address via DHCP.

Syntax

1. Enabling the DHCP proxy and setting an IP range.

```
config system settings
   set dhcp-proxy enable
   set dhcp-server-ip <IP_address>
   set dhcp6-server-ip <IP_address>
end
```

2. Setting the IPsec phase one to assign IP addresses using the DHCP proxy.

```
config vpn ipsec phase1
   edit <id>
      set assign-ip-from dhcp
   end
end
```

IP assignment can also come from a locally defined range or via the user group.

Transform Matching

FortiOS 5.2 supports combining multiple encryption, authentication, PRF, and DH transforms in a single IKEv2 proposal, which is used for selecting a transform set when the FortiGate unit is the responder. Each proposal now holds lists of transforms, instead of having just a single value per transform type. When negotiating, the proposal iterates over the transform lists to find a match.

Cookie Notification

Upon detecting that the number of half-open IKEv2 SAs is above the threshold value, the VPN dialup server will require all future SA_INIT requests to include a valid cookie notification payload that the server sends back, in order to preserve CPU and memory resources.

Message ID Sync for High Availability

IKE Message ID Sync is supported in FortiOS 5.2. Message ID Sync allows IKEv2 to re-negotiate send and receive message ID counters after a high availability fail over. By doing this, the established IKE SA can remain up, instead of re-initializing.

A diagnose command has also been added to show statistics for the number of HA messages sent/received for IKE: `diagnose vpn ike ha stats`.

Dynamic IPsec Route Control

Greater control has been added in FortiOS 5.2 concerning adding routes for IPsec VPN.

add-route

The `add-route` option is now available for all dynamic IPsec phase 1s and phase 2s, for both policy-based and route-base IPsec VPNs. This allows you to control the addition of a route to a peer destination selector.

This option was previously only available when `mode-cfg` was enabled in phase 1. Also, in phase 2, a new option has been added allowing `add-route` to automatically match the settings in phase 1.

This feature is enabled by default.

Syntax

1. Configuring phase 1:

```
config vpn ipsec {phase1 | phase1-interface}
   edit <name>
      set type dynamic
      set add-route {enable | disable}
   end
```

2. Configuring phase 2:

```
config vpn ipsec {phase2 | phase2-interface}
   edit <name>
      set add-route {phase1 | enable | disable}
   end
```

Blocking IPsec SA Negotiation

For interface-based IPsec, IPsec SA negotiation blocking can only be removed if the peer offers a wildcard selector. If a wildcard selector is offered then the wildcard route will be added to the routing information base with the distance/priority value configured in the phase1 and, if that is the route with the lowest distance, it will be installed into the forwarding information base.

In a case where this occurs, it is important to ensure that the distance value on the phase1 is set appropriately.

Default Lifetimes and Proposal Values

The default lifetimes for IKE and IPsec have been lengthened in FortiOS 5.2. The number of proposals has also increased and new default proposals have been created for Phase 1 and Phase 2. The changes are as follows:

- The default Phase1 lifetime is 86400 seconds (1 day).
- The default Phase2 lifetime is 43200 seconds (12 hours).
- The default Phase1 proposals are: aes128-sha256, aes256-sha256, 3des-sha256, aes128-sha1, aes256-sha1, and 3des-sha1.
- The default Phase2 proposals are: aes128-sha1, aes256-sha1, 3des-sha1, aes128-sha256, aes256-sha256, and 3des-sha256.
- The maximum number of proposals has been increased from 3 to 10.
- The default Diffie-Hellman (DH) group for phase1 and phase2 has changed from 5 to 14.

Prioritizing DH Group Configuration

In FOS 5.2, the default Diffie-Hellman DH group has changed from 5 to 14, to provide sufficient protection for stronger cipher suites that include AES and SHA2. Because of this change, both IKEv1 and IKEv2 now allow up to 3 DH groups to be configured in the phase 1 and phase 2 settings, while preserving the ordering since the initiator always begins by using the first group in the list. The default DH group in the configuration has been updated to include group 14 and 5, in that order. You can add and remove other groups and the order they appear in the configuration is the order in which they are negotiated.

The IKEv1 protocol does not natively provide for DH group negotiation in Aggressive Mode and Quick Mode. As a result, when multiple DH groups are used with IKEv1 Aggressive Mode or Quick Mode, delays in tunnel establishment can occur and so it is recommended to continue to configure matching DH groups on both peers whenever possible.

During negotiation with multiple DH groups, the new operation is as follows:

1. **IKEv1 Aggressive Mode Initiator:** Since Aggressive Mode includes the KE payload in the first message, FortiOS must select a group to use to generate the DH public number. FortiOS starts with the first group in the list. If the negotiation fails due to timeout, it will try the second group, and finally the third. If the third also fails, FortiOS goes back to the first DH group again, and starts over. Once it finds the correct group and the tunnel is established, it will continue to use that group for re-keying as long as the VPN connection remains up.
2. **IKEv1 Aggressive Mode Responder:** If the group proposed by the initiator doesn't match the group proposed by the responder, the negotiation fails due to no proposal chosen. Since authentication has not been established the responder cannot send a notify message to the initiator. The initiator will try the next DH group in its configuration when the negotiation time out occurs, which takes 30 seconds by default. At that point, if the next DH group is a successful match, the tunnel comes up.
3. **IKEv1 Main Mode Initiator:** In Main Mode, the SA and KE payloads come in different messages. The SA parameters, including DH group, are negotiated first in MM1 and MM2, then the KE payloads are exchanged in the MM3 and MM4 messages. So no change was made for Main Mode.
4. **IKEv1 Main Mode Responder:** As above, no change for Main Mode.
5. IKEv1 Quick Mode Initiator: Quick Mode has the same problem as Aggressive Mode, in that the SA proposal and KE payloads arrive in the same message. So unlike Main Mode, the initiator does not know the negotiated DH group prior to constructing its KE payload. Like with AM, it will start with the first group in the configured DH group list. If the negotiation times out, or if we receive a No-Proposal-Chosen notify message from the responder, we will switch to the next group in the list and try again.
6. IKEv1 Quick Mode Responder: Similar to Aggressive Mode, if the initiator's first group doesn't match, the Quick Mode will fail with a no proposal chosen error. In Quick Mode, you have the benefit of an authenticated IKE SA by which you can immediately notify the peer of the error. Sending the No-Proposal-Chosen notify to the initiator allows the initiator to try the next group immediately without waiting for a timeout.
7. **IKEv2 SA_INIT/CHILD_SA Initiator:** Like Aggressive Mode, in IKEv2 both the SA_INIT and CHILD_SA exchanges have the SA proposal and KE payload in the same message. However, unlike IKEv1, the IKEv2 RFC specifies a mechanism to handle this. In IKEv2, if the negotiated DH group does not match the group specified in the KE payload, the INVALID_KE notify message is sent and the initiator retries the exchange using the DH group specified in the notify message. Initiator side support for handling the INVALID_KE message has been added. This code wasn't needed previously, as the IKEv2 CLI allowed only one DH group to be configured. Now that the CLI restriction has been removed and multiple DH groups can be configured for IKEv2 in the phase1 and phase2 settings, the initiator will handle receipt of INVALID_KE messages as per the IKEv2 RFC. As long as the VPN connection remains up, the initiator will subsequently re-key using the negotiated group.
8. **IKEv2 SA_INIT/CHILD_SA Responder:** The responder side of our IKEv2 code already supports handling of the INVALID_KE message.

IPv6 Support for IPsec Phase 2

IPv6 support has been added to IPsec phase 2, allowing IPv6 firewall address and address groups to be used for phase 2 source and destination address types. The management of static selector rules has also been moved into the IKE daemon, allowing named selectors to be reloaded if any named address or address groups are changed, without requiring the FortiGate unit to be rebooted before changes are applied.

IPsec VPN Support with the FortiController-5103B

The FortiController-5103B can now learn the routing table as a slave to receive the update from master. When packets are received, the 5103B blade tests the routing table to determine whether the traffic will be routed to the IPsec interface, if it does, it will trigger 5103 to forward the traffic to dedicated IPsec blade. This ensures that all IPsec traffic is sent to the dedicated IPsec blade, even traffic originating from the 5000 system, such as monitoring systems or internal emails.

SSL VPN

New SSL VPN features include:

- SSL VPN Configuration
- ECDSA Local Certificates
- Host Security Check Error Replacement Message

SSL VPN Configuration

Several changes have been made to how SSL VPNs are created and configured.

VPN Settings

The SSL VPN settings page, found at **VPN > SSL > Settings**, has been reorganized to be more intuitive. The settings are now found in the following sections:

- **Connection Settings** define how users connect and interact with an SSL VPN portal. This section includes Listen on Interface(s), Idle Logout, and Server Certificate.
- **Tunnel Mode Client Settings** define the settings that clients will receive upon connecting to the VPN. This section includes Address Range and Allow Endpoint Registration.
- **Authentication/Portal Mapping** allows you to define different portals to different users and groups.

VPN Portal

New options for split tunneling have been added to SSL VPN portals, which are configured by going to **VPN > SSL > Portals,** including a routing address and a tunnel mode for IPv6. These options can also be configured in the CLI, using the command `config vpn ssl web portal`.

Creating the Firewall Policy

When creating a firewall policy for your SSL VPN, you will select ssl.root as the **Incoming Interface**. Also, source devices are not applicable to SSL VPN firewall policies.

For more information about using a virtual WAN link, please see the FortiGate Cookbook recipe SSL VPN for Remote Users.

ECDSA Local Certificates

The use of ECDSA Local Certificates for SSL VPN Suite B support is now supported. This will allow the following:

1. Importing ECDSA certificate.
2. Generating ECDSA certificate requests.
3. Using ECDSA certificate in SSL VPN.
4. Using ECDSA certificate in web-based manager.

ECDSA certificates can be generating using the following command in the CLI: `exec vpn certificate local generate ec`.

RSA certificates are now generated using the following command:

```
exec vpn certificate local generate rsa.
```

Host Security Check Error Replacement Message

The replacement message that now appears when an SSL VPN host security check fails can now be customized using the CLI.

Syntax

```
config system replacemsg sslvpn hostcheck-error
   set buffer <string>
   set header {none | http | 8bit}
   set format {none | text | html}
end
```

Authentication

New authentication features include:

- Captive Portal
- User Authentication via a POP3 Server
- Limiting Guest User Accounts
- Nested Group Search in LDAP Authentication
- Password Length for User Authentication
- Certificates for Policy Authentication
- Authentication Blackouts
- Single Sign-On for Guest Accounts

Captive Portal

There have been several changes made to authentication using a captive portal. Additional captive portal options have also been added for wireless networks. For more information, see Captive Portal for WiFi on page 142.

External Captive Portals

An external captive portal can be used to configure each FortiGate interface as an independent, external web URL. To configure an interface, go to **System > Network > Interfaces** and edit the desired interface. Select **Captive Portal** as the **Security Mode**, then set **Authentication Portal** to **External** and configure the other settings as required.

Once a client has been authenticated by the portal, by default they will be sent to original URL that was requested. The portal can also be configured to send the client to a hard coded URL that contains a replacement message.

Syntax

In the following example, the LAN interface is configured with external captive portal that has a specified URL (http://10.6.2.218/?Auth=Success) to redirect clients to after successful authentication.

```
config system interface
   edit "lan"
      set security-mode captive-portal
      set security-external-web "http://10.6.2.218/portal"
      set security-redirect-url "http://10.6.2.218/?Auth=Success"
      set security-groups "rug1"
   end
```

Using Groups from the Security Policy

Portal interfaces can now be configured to use the user groups set in the security policies. This will happen by default if no user group is configured on the interface.

Exempting a Policy

Security policies can now be exempt from captive portals, using the command `captive-portal-exempt enable`.

Replacement Messages

The captive portal-specific replacement messages have been removed. Authentication replacement messages will be used for portals.

User Authentication via a POP3 Server

A POP3 server can now be used to verify user credentials when they authenticate through a web portal or any supported authentication method.

The following maximum values are associated with POP3 authentication:

- A maximum of 10 pop3/pop3s servers can be defined per box
- A single user group can have up to a pool of 6 POP3 servers assigned

POP3 authentication can be configured using the CLI:

Configuring a POP3 user

```
config user pop3
   edit name
      set server "pop3.fortinet.com"
      set secure {starttls | pop3s | none}
      set port 110
   end
```

Configuring a POP3 user group

```
config user group
   edit pop3_grp1
      set member "pop3_server1" "pop3_server2"
   end
```

Limiting Guest User Accounts

A new option to has been added to the guest user group where the administrator can restrict the maximum number of guest accounts that can be created. After the limit is reached, the portal administrator will need to remove some expired accounts. The number of accounts can be set from 1-1024 or left as unlimited (0 in the CLI), which is the default setting.

In the web-based manager, the lower limit is restricted if there are existing group members. In order to set a lower number, guest accounts must be removed prior to the limit being set.

Syntax

```
config user group
   edit guest-group
```

```
      set group-type guest
      set max-accounts [0-1024]
   end
```

Nested Group Search in LDAP Authentication

Nested group search is a new feature added to Windows AD server when the LDAP server's settings have `group-member-check` set to `user-attr`. After authentication succeeds, `fnbamd` gets groups from user attributes and repeats LDAP queries on the groups until reaches the top layer.

Syntax

```
config user ldap
   edit <ldap-server-name>
      set search-type nested
   end
```

Password Length for User Authentication

In FortiOS 5.2, the length for all passwords connected to user authentication features has been changed to support a maximum of 128 characters.

Certificates for Policy Authentication

The CA certificate used for policy authentication can now be configured, instead of being restricted to the built-in Fortinet certificate. By doing this, the authenticated user can be presented with a certificate that is already trusted by their browser and certificate errors can be avoided.

Syntax

```
config user setting
   set auth-ca-cert <name>
end
```

Authentication Blackouts

If five failed logins are made from an IP within one minute, the IP is put on a blackout list. Future logins from this IP are rejected as long as the IP is on this list. The IP remains on the blackout list for auth-blackout-time seconds. The amount of time an IP is blacklisted can be configured through the CLI:

Syntax

```
config user setting
   set auth-blackout-time 300
end
```

This feature only applies to IP-based authentication schemes.

Single Sign-On for Guest Accounts

The default **FSSO_Guest_Users** group has changed to **SSO_Guest_Users**. This group supports guests using both Fortinet Single Sign-On (FSSO) and RADIUS Single Sign-On (RSSO). Users can also now be added to this group SSO_Guest_group using the CLI.

Syntax

```
config user group
   edit SSO_Guest_group
      set member <names>
   end
end
```

Managing Devices

New device management features include:

- On-Net Status for FortiClient Devices
- Endpoint Licenses
- URL Filter Lists in Endpoint Control
- FortiGuard Categories Consistency with FortiClient
- Default Device Groups
- Device Detection for Traffic Not Flowing Through the FortiGate

On-Net Status for FortiClient Devices

The **Online** column of the FortiClient Monitor has been changed to **Status**. This column will show the current status of the device, and whether or not it is registered.

Two of the possible status options are on-net or off-net. In order to record this information, the DHCP server must be enabled for FortiClient On-Net Status. In order to determine if a FortiClient device is on or off net, a DHCP cookie is sent to FortiClient that contains the FortiGate's serial number. FortiClient will then compare that serial number to the number for the FortiGate it is registered with. If they match, the FortiClient will be considered on-net.

In configurations using high availability, the cookie contains the serial number of all cluster members.

This status has also led to the following options have been added to FortiClient profiles:

- Client Web Filtering when On-Net: when enabled, web filtering is applied to FortiClient traffic even when it is protected by a FortiGate unit.
- Auto-connect when Off-Net: This option allows the FortiClient to autoconnect to a VPN even when it has an off-net status.
- Client-based Logging when On-Net: when enabled, the FortiClient will continue to log even when its traffic is flowing through a FortiGate unit.

Endpoint Licenses

New Endpoint licenses are now available in FortiOS 5.2. Information about the status of the current license can be found in the FortiClient section of the **License Information** widget.

The following licenses will be available:

- **Desktop models and FortiGate-VM00:** 200 clients
- **1U models, FortiGate-VM01 and FortiGate-VM02:** 2,000 clients
- **2U models and FortiGate-VM04:** 8,000 clients
- **3U models, FortiGate-ATCA, and FortiGate-VM08:** 20,000 clients

Because the new licenses are for one year, the activation method has changed. New licenses are purchased similarly to a FortiGuard service, with no further registration of the license required. The device can then be registered with the FortiGate unit.

If the device does not have access to Internet, you can download the license key from support site and manually upload it to your FortiGate. The license will be for that specific device and will have an license expiry date.

While the older licenses from FortiOS 5.0 will still be supported, they will have the following limitations:

- The On-Net Status feature will not be supported.
- Logging options will only appear in the CLI.
- FortiAnalyzer Support for logging and reporting will be limited.
- You will not be able to enter any v5.0 license keys.

URL Filter Lists in Endpoint Control

URL filters can now be sent to devices running FortiClient that connect to the FortiGate unit. All URL filter types (Simple/Regex/Wildcard) and actions (Allow/Block/Exempt/Monitor) can be deployed to FortiClient

Upon receiving the URL filter list, FortiClient will save and display the received URL filter list in the web-based manager.

If the URL list is later changed or removed from the FortiGate unit, these changes will also appear in FortiClient.

FortiGuard Categories Consistency with FortiClient

If FortiGuard categories are disabled on a FortiGate unit, they will now also be disabled in FortiClient for managed devices, even if FortiGuard categories were used previously.

Default Device Groups

The predefined device groups have been changed to the following:

- Windows PC (includes Windows servers and computers but not tablets or phones)
- Mac
- Linux
- Printer
- Mobile devices (includes tablets and phones from all vendors)
- VoIP phones
- Router/firewall/gateway devices (does not include switch devices)
- Other (for unknown devices)

To improve accuracy, device types are now identified using UIDs instead of MAC addresses.

Device Detection for Traffic Not Flowing Through the FortiGate

In FortiOS 5.2, any traffic hitting a FortiGate interface, regardless of whether it is going to be dropped, forwarded or processed locally, will be used by device detection, allowing devices to be detected even if their traffic does not flow through the FortiGate unit. This includes traffic that hits an interface with IPS sniffer mode enabled, as well as broadcast and multicast traffic.

Wireless Networking

New wireless networking features include:

- FortiAP Management
- Captive Portal for WiFi
- New Wireless Health Charts
- RADIUS Accounting
- 802.11ac and DARRP Support
- Date Channel DTLS in Kernel

FortiAP Management

How FortiAP units are managed by a FortiGate unit has changed in several ways.

Manually Selecting AP Profiles

AP profiles are no longer assigned automatically. Instead, a default or custom profile must be chosen when the connection to the FortiAP unit is configured.

The **Background Scan** option has also been replaced by **Spectrum Analysis** (for more information, see New Wireless Health Charts) and either 20MHz or 40MHz must be selected for Radio 1's channel width.

You can choose to override some options set in the profile for a particular FortiAP unit. To do this, go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and, under **Wireless Settings**, select **Override Settings**. This allows you to change WiFi radio settings, including SSIDs, TX power, and rogue AP scanning. This can also be configured in the CLI:

Syntax

```
config wireless-controller wtp
   edit <name>
      set override-profile enable
   end
end
```

AP Scanning

AP scanning, including rogue AP detection, is now part of WIDS Profiles. It can be found by going to **WiFi Controller > WiFi Network > WIDS Profiles**. It can also be configured through the CLI:

Syntax

```
config wireless-controller wids-profile
   edit 0
      set ap-scan {enable | disable}
      set ap-bgscan-period <interval>
      set ap-bgscan-intv <interval>
      set ap-bgscan-duration <interval>
      set ap-bgscan-idle <interval>
      set ap-bgscan-rpot-intv <interval>
```

```
      set ap-bgscan-disable-day <day>
      set ap-fgscan-repot-intv <interval>
      set rogue-scan {enable | disable}
    end
end
```

Radio Settings Summary

The Radio Settings Summary table can be found by going to **WiFi Controller > Managed Access Points > Managed FortiAPs** and editing a FortiAP unit. The table shows information on the FortiAP unit's Radio 1 and 2 (if applicable), including settings, channels, and SSIDs.

CLI Console Access

The CLI console on a FortiGate unit can now be used to connect directly to a managed FortiAP unit that has been configured to enable login-enable. To access the FortiAP, use the command `execute telnet <ip>`, using the IP address of the FortiAP.

Telnet must be used, as FortiAPs do not support SSH/HTTPS admin access.

The console can also now be accessed by going to **WiFi Controller > Managed Access Points > Managed APs** and selecting the option **Connect to CLI**. The console will appear in a pop-up window.

If `login-enable` is set to `default` or `disable` on the FortiAP unit, or the FortiAP is offline, this option will not appear.

Split Tunneling for Wireless Traffic

Split tunneling can now be used for wireless traffic, allowing you to optimize WiFi traffic flow by directing only corporate traffic back to the FortiGate unit's wireless controller, while local application traffic remains local. With split tunneling, a remote user associates with a single SSID, can get access to corporate resources (for example, a mail server) and local resources (for example, a local printer).

Split tunneling should be only used for SSIDs in tunnel mode.

Syntax

1. Enabling split tunnelling for an SSID.

```
config wireless-controller vap
   edit <name>
      set split-tunneling enable
   end
end
```

2. Setting the IP lists for split tunneling

```
config w-c {wtp-profile | wtp}
   set split-tunneling-acl-local-ap-subnet enable
   config split-tunneling-acl
      edit <ID>
```

```
            set id <ID>
            set dest-ip <IP_address>
        end
    end
```

Captive Portal for WiFi

Several changes have been made for captive portal security on wireless networks. Wireless captive portals can also use the new features for all captive portals described in "Authentication" on page 134.

New Configuration Options

The following options can now be configured for captive portals that use wireless interfaces:

- Security exempt list names can be added to a captive portal. This option is only available when user groups are selected as part of the SSID configuration, rather than being a match for groups in the security policy.
- URL redirection is available after the disclaimer/authentication screen.
- Four types of portals are available: authentication, authentication with disclaimer, disclaimer only, or email collection. When the mode is email collection or disclaimer only, the options for setting user groups or having an external captive portal are not available.

Syntax

```
config wireless-controller vap
   edit <name>
      set security captive-portal
      set portal type {auth | auth+disclaimer | disclaimer | email-collect}
      set security-exempt-list <name of list>
   end
end
```

WPA Personal Security + Captive Portal

A new option has also been added that uses WPA Personal security as well as a captive portal. This option also allows groups to be imported from the policy.

New Wireless Health Charts

Two new charts have been added to the Wireless Health Monitor showing spectrum analysis information on the sources of wireless interference.

In order for these widgets to appear, spectrum analysis must first be enabled. This is done by editing the AP profile used by your FortiAP units and selecting **Spectrum Analysis** for all applicable radios.

Spectrum analysis can also be enabled in the CLI.

Syntax

```
config wireless-controller wtp-profile
   edit <name>
      config <radio>
         set spectrum-analysis enable
      end
   end
end
```

After spectrum analysis has been enabled, view the **Top Wireless Interference** widget found in the Wireless Health Monitor. A chart icon will appear in the **Channel** column. Selecting this icon will open the new WiFi charts: **Spectrum Analysis** and **Top Wireless Interference**.

The **Spectrum Analysis** chart shows WiFi signal interference as detected by a particular FortiAP.

The **Top Wireless Interference** chart shows SSIDs that are interfering with a particular FortiAP unit.

RADIUS Accounting

RADIUS accounting is now supported for wireless networks, allowing RADIUS accounting messages to be sent that contain a wireless user's name and IP address.

If an accounting server has been enabled for RADIUS, the wireless client information will be sent to it.

802.11ac and DARRP Support

802.11ac support has been added for FortiOS 5.2, allowing a FortiGate unit to manage FortiAP models 221C and 320C. Distributed Automatic Radio Resource Provisioning (DARRP) is also supported for 802.11ac radio.

Syntax

```
config wireless-controller wtp-profile
   edit {fap221c | fap320c}
      config radio-2
         set darrp enable
      end
end
```

Date Channel DTLS in Kernel

Data channel Datagram Transport Layer Security (DTLS) can now be enabled in kernel using the CLI.

Syntax

```
config wireless-controller wtp-prof
   edit wtpprof
      set dtls-in-kernel enable
   end
end
```

IPv6

New IPv6 features include:

- IPv6 Address Ranges
- TCP MSS Values
- RSSO Support
- FortiManager Connections
- Geographical Database

IPv6 Address Ranges

IPv6 address ranges can now be created, using either the web-based manager or the CLI.

Syntax

```
config firewall address6
   edit <name>
      set type iprange
      set start-ip <address>
      set end-ip <address>
   end
end
```

TCP MSS Values

TCP MSS values for both the sender and the receiver can now be set for IPv6 policies using the CLI.

Syntax

```
config firewall policy6
   edit <index_int>
      set tcp-mss-sender <value>
      set tcp-mss-receiver <value>
   end
end
```

RSSO Support

RADIUS Single Sign-On (RSSO) is supported in IPv6 and can be configured in the CLI. Fallthrough for unauthenticated

Syntax

```
config firewall policy6
   edit <id>
      set rsso enable
      set fall-through-unauthenticated enable
   end
end
```

FortiManager Connections

IPv6 can now be used to connect a FortiGate unit to a FortiManager unit.

Geographical Database

An IPv6 geographical database has been added to properly identify the geographical locations of traffic in reports.

High Availability

New high availability features include:

- DHCP and PPPOE Support for Active-Passive Mode
- VRRP Support
- Trigger Failover
- Synchronizing a GTP Tunnel over Physical Ports
- IPv6 Management Interface Gateway

DHCP and PPPOE Support for Active-Passive Mode

High Availability is now supported in Active-Passive mode when there are interfaces working in DHCP client or PPPOE client mode.

VRRP Support

Additional features have been added to support Virtual Router Redundancy Protocol (VRRP).

VRRP Groups

A VRRP group includes all the relevant VRRP IDs and tracks the VRRP status in order to force the status of all group members if a VRRP domain is changed from master to backup.

VRRP groups are configured through the CLI. The VRRP group ID can be between 1 and 65535.

Syntax

```
config system interface
   edit <port>
      config vrrp
         edit <id>
            set vrgrp <id>
         end
   end
```

A **VRRP** column has also been added to the interfaces list in the web-based manager that will show the VRRP ID, group, and status. This list can be found at **System > Network > Interfaces**.

Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down. A second VRDST can be configured using the CLI.

Syntax

```
config system interface
   edit <interface>
      config vrrp
         edit <id>
```

```
            set vrdst <ip1> <ip2>
        end
    end
```

Trigger Failover

HA failover can now be enabled and disabled using the following CLI commands:

- `diagnose sys ha set-as-master enable`: immediately enables the local FortiGate unit as the HA master.
- `diagnose sys ha set-as-master disable`: immediately disables this mode. Optionally, a time frame can be added after `disable`, which will disable the mode at the appointed time. The time format is yyyy-mm-dd hh:mm:ss.

Synchronizing a GTP Tunnel over Physical Ports

In order to properly handle GPRS Tunneling Protocol (GTP) synchronization under high stress loads, FortiOS 5.2 will use the interfaces set in `set session-sync-dev` (part of `config system ha`) to allow GTP tunnels to synchronize directly over physical ports when both the HA primary and secondary are up. A new diagnose command, `diagnose firewall gtp hash-stat`, has also been added to display GTP hash stat separately.

IPv6 Management Interface Gateway

IPv6 management interface gateways are now supported in FortiOS 5.2.

Syntax

```
config system ha
   set ha-mgmt-interface-gateway6 <IPv6_address>
end
```

WAN Optimization, Web Cache, and Explicit Proxy

New WAN optimization, web cache, and explicit proxy features include:

- Explicit Proxy Policy Table - for explicit web proxy, explicit FTP proxy and WAN optimization policies
- Distributing Explicit Web Proxy Traffic to Multiple CPU Cores
- Proxy Header Control
- Explicit Web Proxy SOCKS services support for TCP and UDP traffic
- Preventing the explicit web proxy from changing source addresses
- Explicit web proxy firewall address URL patterns

Explicit Proxy Policy Table - for explicit web proxy, explicit FTP proxy and WAN optimization policies

Explicit proxy policies now have a dedicated table and creation page, found at **Policy & Objects > Policy > Explicit Proxy**. The corresponding CLI command is:

```
config firewall explicit-proxy-policy
```

You use explict proxy policies to add policies for the IPv4 and IPv6 explicit web proxy and for the explicit FTP policy. The first step in creating an explicit proxy policy is to select the proxy type (web or FTP). The options availabl e then depend on the explicit proxy type.

From the CLI you use the explicit web proxy policy to add WAN optimization tunnel policies. In FortiOS 5.0 you added WAN optimization tunnel policies by setting the source interface to wanopt. In FortiOS 5.2 you create an explicit web proxy policy from the CLI and set the proxy type to wanopt. For example:

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf internal
      set srcaddr all
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
   next
end
```

Distributing Explicit Web Proxy Traffic to Multiple CPU Cores

To improve explicit web proxy performance, FortiOS 5.2 distributes explicit web proxy processing to multiple CPU cores. By default web proxy traffic is handled by half of the CPU cores in a FortiGate unit, so if your FortiGate unit has 4 CPU cores, by default two will be used for explicit web proxy traffic. You can increase or decrease the number of CPU cores that are used in the CLI.

```
config system global
   set wad-worker-count <number>
end
```

The value for <number> can be anything between 1 and the total number of CPU cores in your FortiGate unit. The default value for <number> is half the number of CPU cores in your FortiGate unit.

Proxy Header Control

You can create explicit web proxy profiles that can add, remove and change HTTP headers. The explicit web proxy profile can be added to a web explicit proxy policy and will be applied to all of the HTTP traffic accepted by that policy.

You can change the following HTTP headers:

- client-ip
- via header for forwarded requests
- via header for forwarded responses
- x-forwarded-for
- front-end-https

For each of these headers you can set the action to:

- Pass to forward the traffic without changing the header
- Add to add the header
- Remove to remove the header

You can also configure how the explicit web proxy handles custom headers. The proxy can add or remove custom headers from requests or responses. If you are adding a header you can specify the content to be included in the added header.

Create web proxy profiles from the CLI:

```
config web-proxy profile
   edit <name>
      set header-client-ip {add | pass | remove}
      set header-via-request {add | pass | remove}
      set header-via-response {add | pass | remove}
      set header-x-forwarded-for {add | pass | remove}
      set header-front-end-https {add | pass | remove}
         config headers
            edit <id>
               set action {add-to-request | add-to-response | remove-from-request |
                   remove-from-response}
               set content <string>
               set name <name>
            end
      end
```

Use the following command to add a web proxy profile to an explicit proxy policy:

```
config firewall explicit-proxy-policy
   edit <id>
      set webproxy-profile <name>
   end
```

Explicit Web Proxy SOCKS services support for TCP and UDP traffic

You can now configure Web Proxy services to allow UDP traffic as well as TCP traffic to be accepted by the SOCKS proxy. Previously, the web proxy would only accept TCP SOCKS traffic.

Web proxy services can be configured in the CLI.

Syntax

Use the following command to create a custom service for UDP traffic over the SOCKS proxy:

```
config firewall service custom
   edit <name>
      set explicit-proxy enable
      set category Web\ Proxy
      set protocol SOCKS-UDP
      set tcp-portrange 8080-8080
   end
end
```

The option to create a custom service for TCP traffic over the SOCKS proxy has also changed. For example, use the following command to create a custom service for TCP traffic over the SOCKS proxy:

```
config firewall service custom
   edit <name>
      set explicit-proxy enable
      set category Web\ Proxy
      set protocol SOCKS-TCP
      set tcp-portrange 80-80
   end
end
```

Preventing the explicit web proxy from changing source addresses

By default in NAT/Route mode the explicit web proxy changes the source address of packets leaving the FortiGate to the IP address of the FortiGate interface that the packets are exiting from. In Transparent mode the source address is changed to the management IP.

This configuration hides the IP addresses of clients and allows packets to return to the FortiGate unit interface without having to route packets from clients. You can use the following command to configure the explicit web proxy to keep the original client's source IP address:

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set transparent enable
   end
```

Explicit web proxy firewall address URL patterns

You can add URL pattern addresses and address groups to control the destination URLs that explicit web proxy users can connect to. To add a URL pattern to go to **Policy & Objects > Objects > Addresses**, select **Create New** and set the Type to **URL Pattern (Explicit Proxy)**. Add a URL or URL pattern that defines the URL or URLs that explicit proxy users should be limited to. Set the **Interface** to **any**.

For example to limit access to a single website:

www.fortinet.com

To limit access to websites from the same domain:

google.com

To limit access to a part of a website:

www.apple.com/ipad/

To add a URL pattern group, create several URL pattern addresses then go to **Policy & Objects > Objects > Addresses**, select **Create New > Group** and add URL patterns to the address group.

Then when creating explicit web proxy policies, select the URL pattern addresses or groups as the destination address.

URL patterns and HTTPS scanning

For HTTPS traffic, URL patterns can only be matched up to the root path. For example, consider the following URL pattern:

www.apple.com/ipad/

If a proxy user browses using HTTP, this URL pattern limits their access the iPad pages of www.apple.com. However, if a proxy user browses using HTTPS, they will be able to access all pages on www.apple.com.

Advanced Routing

New advanced routing features include:

- BGP Neighbor Groups
- OSPF Fast Hello
- BGP Conditional Advertising
- Source and Destination IP-based Mode for ECMP
- Policy Routes

BGP Neighbor Groups

A Border Gateway Protocol (BGP) neighbor group can now be configured automatically based on a range of neighbors' source addresses, rather than configuring neighbors individually. A maximum number of neighbors can be set for each group to be between 1 and 1000.

Syntax

```
config router bgp
   config neighbor-group
      edit <name>
         set ... (same configuration options as config neighbor)
   next
   config neighbor-range
      edit <id>
         set prefix <class_ip&net_netmask>
         set max-neighbor-num <integer>
         set neighbor-group <name>
      end
end
```

OSPF Fast Hello

Open Shortest Path First (OSPF) fast hello provides a way to send a set number of hello packets per second and use a dead interval of four hellos. Fast hello can be configured on an OSPF interface through the CLI. If `dead-interval` is set to 1 second, fast hello will be enabled. The `hello-multiplier` value, which can be between 4 and 10, sets the number of hello packets that will be sent per second.

Syntax

```
config ospf-interface
   edit ospf1
      set interface port1
      set network-type broadcast
      set dead-interval 1
      set hello-multiplier 4
   end
end
```

BGP Conditional Advertising

BGP conditional advertising is supported in FortiOS 5.2.

Normally, routes are propagated regardless of the existence of a different path. Using BGP conditional advertisement allows a route not to be advertised based on existence or non-existence of other routes. With this new feature, a child table under bgp neighbor is introduced. Any route matched by one of the route-map specified in the table will be advertised to the peer based on the corresponding condition route-map.

Syntax

```
config router bgp
   config neighbor
      edit <name>
         set remote-as 3
         config conditional-advertise
            edit <name>
               set condition-routemap <name>
               set condition-type {exist | non-exist}
            end
         end
      end
   end
end
```

Source and Destination IP-based Mode for ECMP

A new mode has been added that allows Equal-cost multi-path routing (ECMP) to select next hop based on both source and destination IPs. This can be configured as a global setting (if `virtual-wan-link` is disabled) or for a virtual WAN link.

Syntax

```
config system {settings | virtual-wan-link}
   set v4-ecmp-mode source-dest-ip-based
end
```

Policy Routes

The following options have been added for policy routes:

- Multiple source/destination subnets.
- Multiple input devices.
- `src-negate` and `dst-negate` can now be enabled.
- `action` can now be set to `permit` or `deny`.

Logging and Reporting

New logging and reporting features include:

- Traffic and UTM Logging Improvements
- FortiGate Daily Security Report
- GTP Logging Improvements
- Flash-based Logging Disabled on Some Models
- Accessing Policy-specific Logs from the Policy List
- IPS Event Context Data in Log Messages
- Sniffer Traffic Log
- Selecting Sources for Reports
- Threat Weight
- Disk Usage Information in System Event Logs
- Event Log Generated When a Crash Occurs
- Displaying FortiFlow Names

Traffic and UTM Logging Improvements

Traffic and UTM Logging has been simplified in FortiOS 5.2 by making the following changes:

- Removing all overlapping fields between the UTM Logs and Traffic Logs, with the exception of the common fields `sessionid`, `vd`, `user`, and `group`, and application control critical info, which will be present in both the Traffic Log and Application log.
- Fields have been renamed so that they are the same in all logs.
- Some rarely used fields were removed; for example, `profiletype`.
- The `action` field reflects the Firewall action (accept or deny). This will allow you to see from the traffic logs if the session was allowed or blocked and whether it was allowed or blocked by the firewall or by a security feature. If it was a security feature, you will need to look at the UTM logs to determine which feature blocked the traffic.
- The field `utmaction` is set to the most severe actions across all security features. The severity from highest to lowest is: Block, Reset, Traffic Shape, Allow.
- You can now drill-down from a traffic log to its corresponding UTM logs.
- `extended-utm-log` and `log` options for security profiles have been removed.
- Log roll logic have been rewritten so that traffic log file and related utm log files are rolled together. Uploadd will pack these files together to send to a FortiAnalyzer unit.
- An anomaly log category has been added to separate anomaly logs from IPS logs.

FortiGate Daily Security Report

The FortiGate UTM Security Analysis Report has been renamed the FortiGate Daily Security Report.

A variety of other changes have also occurred to the report:

- A new cover page has been added that contains the report name, date, date range, and device name.
- A table of contents page has been added.

- The information VPN usage now shows all use, rather than just a top 10 list. This allows a complete list to be shown that includes all tunnels for Site-to-Site IPsec VPNs and all users for dial-up IPsec VPN tunnels, SSL VPN tunnels, and SSL VPN web mode. Information on connection time has also been added.
- Entries will not be displayed when there is a zero bandwidth/or connection time.

GTP Logging Improvements

Several changes have been made concerning GPRS Tunneling Protocol (GTP) and logging.

GTP-U Logging

FortiOS 5.2 supports GPRS Tunnelling Protocol User Plane (GTP-U) logging for both forwarded and dropped packets at the kernel level. FortiGate log entries now contain International Mobile Subscriber Identity (IMSI), Mobile Subscriber Integrated Services Digital Network-Number (MSISDN), Access Point Name (APN), and header Tunnel Endpoint Identifier (TEID) if available/applicable.

Three new CLI commands are added to GTP profile for GTP-U logging:

- `gtpu-forwarded-log`: Enable/disable logging of forwarded GTP-U packets.
- `gtpu-denied-log`: Enable/disable logging of denied GTP-U packets.
- `gtpu-log-freq`: Sets the logging frequency of GTP-U packets.

Syntax

```
config firewall gtp
   edit gtp_profile
      set gtpu-forwarded-log enable
      set gtpu-denied-log enable
      set gtpu-log-freq 10
   end
end
```

The log frequency value is per number of packets, for example `set gtpu-log-freq 10` means the FortiGate unit should have a log entry per 10 packets.

GTP Event Log

A new GTP event log has been added, which can be found by going to **Logging & Reports > Event Log > GTP**. This log will show GTP activity status and a Deny Cause for any traffic that was blocked or dropped.

In order to see this log, it must be enabled either in the Log Settings or in the CLI.

Syntax

```
config log eventfilter
   set gtp enable
end
```

Flash-based Logging Disabled on Some Models

On some FortiGate models, flash-based logging is not available in FortiOS 5.2. For these platforms, Fortinet recommends the free FortiCloud central logging & reporting service, as it offers higher capacity and extends the features available to the FortiGate.

For a full list of affected models, please refer to the Release Notes.

Accessing Policy-specific Logs from the Policy List

In FortiOS 5.2, the log viewer can be opened directly from the policy table, with filters applied automatically to show only the logs relating to that policy. To view these logs, right-click on the **Seq.#** column for the policy and select **Show Matching Logs**.

The log viewer will filter using the Policy UUID if it is enabled. If not, the Policy ID will be used.

IPS Event Context Data in Log Messages

Attack context logging can now be enabled for an IPS sensor, which will add two new fields, `attackcontext` and `attackcontextid`, into an attack log.

The `atkctx` field in log will output BASE64 encoded string of:

```
<PATTERNS> trigger patterns separated by ';' </PATTERNS> <URI> uri buffer </URI>
    <HEADER> header buffer </HEADER> <BODY> body buffer </BODY> <PACKET> packet
    buffer </PACKET>"
```

`Attackcontext` entries longer than 1KB is split in multiple log entries, which share the same `incidentserialno`. `Attackcontextid` will help identify these segment by showing what order they have in the sequence; for example, `<1/3>` means this log is the first segment of a log message containing three segments in total.

Sniffer Traffic Log

Forward traffic from a FortiGate unit that is in one-arm sniffer mode can now be logged on that FortiGate unit. To log this traffic, the appropriate logging option must be selected for the sniffer interface.

Logging information can be viewed in the new sniffer log, which can be found by going to **Log & Report > Forward Traffic > Sniffer Traffic**.

Selecting Sources for Reports

The source for reports can now be configured to be either forward traffic, sniffer traffic, or both.

Syntax

```
config report setting
   set status enable
   set report-source {forward-traffic | sniffer-traffic | both}
end
```

Threat Weight

The 5.0 feature client reputation has been renamed Threat Weight in FortiOS 5.2 and has been moved from Security Profiles to **Log & Report > Log Config > Threat Weight**. It can now be configured in the CLI using the command `config log threat-weight`.

Disk Usage Information in System Event Logs

Disk usage information will now be included in system event logs for FortiGate models that have a hard disk.

Event Log Generated When a Crash Occurs

A brief event log will now be generated when a crash occurs with brief information about the crash.

Displaying FortiFlow Names

Object name data will now be pulled from FortiFlow in applicable locations, including the **Forward Traffic** log and the **Top Destinations** widget.

Other New Features

Other new features in FortiOS 5.2 include:

- SIP Traffic is Handled by the SIP ALG by Default
- Changing the Header Name of Load Balanced HTTP/HTTPS Traffic
- TOS and DSCP Support for Traffic Mapping

SIP Traffic is Handled by the SIP ALG by Default

Previous versions of FortiOS used the SIP session helper for all SIP sessions. You had to remove the SIP session helper from the configuration for SIP traffic to use the SIP ALG.

In FortiOS 5.2, all SIP traffic is now processed by the SIP ALG by default. You can change the default setting using the following command:

```
config system settings
   set default-voip-alg-mode {proxy-based | kernel-helper-based}
end
```

The default is `proxy-based`, which means the SIP ALG is used. If set to `kernel-helper-based`, the SIP session helper is used. If a SIP session is accepted by a firewall policy with a VoIP profile, the session is processed using the SIP ALG even if `default-voip-alg-mode` is set to `kernel-helper-based`.

If a SIP session is accepted by a firewall policy that does not include a VoIP profile:

- If `default-voip-alg-mode` is set to `proxy-based`, SIP traffic is processed by the SIP ALG using the default VoIP profile.
- If `default-voip-alg-mode` is set to `kernel-helper-based`, SIP traffic is processed by the SIP session helper. If the SIP session help has been removed, then no SIP processing takes place.

Changing the Header Name of Load Balanced HTTP/HTTPS Traffic

A header name can now be configured for HTTP and HTTPS traffic that flows through a virtual server, rather than using the default X-Forward-For header.

In order to use this feature, the HTTP IP header must be enabled.

Syntax

```
config firewall vip
   edit <name>
      set type server-load-balance
      set server-type {http | https}
      set http-ip-header enable
      set http-ip-header-name <name>
   end
end
```

TOS and DSCP Support for Traffic Mapping

Both TOS and DSCP are now supported for traffic mapping but only one method can be used at a time, with TOS as the default. The type used and its other attributes can be configured through the CLI.

Syntax

```
config system global
   set traffic-priority {tos | dscp}
   set traffic-priority-level {low | medium | high}
end
```

RFC List

The following RFCs are supported by the new features in FortiOS 5.2:

Number	Title
791	Internet Protocol
1349	Type of Service in the Internet Protocol Suite
1925	The Twelve Networking Truths
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
5996	Internet Key Exchange Protocol Version 2 (IKEv2)

Chapter 2 - Getting Started

This guide contains the following sections:

- Differences between Models examines key types of differences between FortiGate models.
- Installation contains information about installing a FortiGate unit in your network.
- Using the Web-Based Manager contains information about how to use the web-based manager, also known as the GUI.
- A Guide to Using the Desktop Models contains information about using FortiGate models 20-90, also known as the Desktop models.
- Basic Administration contains information about basic tasks that should be done to set-up a new FortiGate unit.
- Next Steps contains a list resources that are available to help you with more advanced FortiGate configurations.

Differences between Models

This section examines some of the key types of differences that exist between different FortiGate models.

Features

There are certain features that are not available on all models. For example, the Switch Controller, which allows a FortiGate unit to manage a FortiSwitch unit, is only available on FortiGate models 100D, 140D, 200D, 240D, 600C, 800C, and 1000C.

Other features may be available only through the CLI on models, while other models have options in the web-based manager. For example, SSL content inspection is a CLI-only feature on FortiGate models 20C, 30C, and 40C, while models 60C+ have options in the web-based manager.

For more information about some of the features that vary by model, please see the Feature/Platform Matrix.

If there is a feature you believe your FortiGate model supports that does not appear in the web-based manager as expected, go to **System > Config > Features** and ensure the feature is turned on. For more information, see Feature settings on page 193.

Names

Naming conventions may vary between FortiGate models. For example, on some models the hardware switch interface used for the local area network is called **lan**, while on other units it is called **internal**.

Menus

Menus may vary by model. For example, on some FortiGate units, the main menu option **Router** is not available. Instead, routing is configured by going to **System > Network > Routing.**

Installation

This section provides information about how to install your FortiGate and use it in your network, after you have finished the initial set-up outlined in the FortiGate model's QuickStart Guide. The section also provides troubleshooting methods to use if the FortiGate does not function as desired after completing the installation.

The following topics are included in this section:

NAT/Route Mode vs Transparent Mode
Installing a FortiGate in NAT/Route Mode
Installing a FortiGate in Transparent Mode
Troubleshooting your FortiGate Installation
Using Port Pairing to Simplify Transparent Mode

NAT/Route Mode vs Transparent Mode

A FortiGate unit can operate in one of two modes: NAT/Route or Transparent.

NAT/Route mode is the most common operating mode. In this mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT). NAT/Route mode is also used when two or more Internet service providers (ISPs) will be used to provide the FortiGate with redundant Internet connections.

A FortiGate unit in Transparent mode is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

Installing a FortiGate in NAT/Route Mode

There are two main types of FortiGate installations using NAT/Route mode: standard installations that receive Internet access from a single Internet service provider (ISP) and installations that have two or more ISPs for redundant Internet connections. For both installations, the first step is to select which internal Switch mode you require your FortiGate to operate in.

Selecting an Internal Switch mode

The internal Switch mode determines how the FortiGate's physical ports are managed by the FortiGate. The two main modes are Switch mode and Interface mode.

Switch mode vs Interface mode

In Switch mode, all of the internal interfaces are part of the same subnet and treated as a single interface, which is called either **lan** or **internal** by default, depending on the FortiGate model. Switch mode is commonly used in settings where the network layout is fairly basic, with most users being on the same subnet.

In Interface mode, the physical interfaces of the FortiGate unit are configured and handled individually, with each interface having its own IP address. Interfaces can be logically or virtually combined by configuring them as part of either hardware or software switches (for more information, see Hardware Switches vs Software Switches on page 165), which allow multiple interfaces to be treated as a single interface. FortiGate units that are in Interface mode by default start with a hardware switch called either **lan** or **internal,** depending on the FortiGate model. This mode is designed for complex networks where different subnets are used to compartmentalize the network traffic.

The default mode that a FortiGate starts in varies depending on the model. Switch mode has been the most common factory default setting; however, the number of models that have Interface mode as their default setting is increasing.

In order to determine which mode your FortiGate unit is in, go to **System > Network > Interfaces.** Locate the interface called either **lan** or **internal**, which all FortiGate units have be default. If the interface is listed as a physical interface in the **Type** column, then your FortiGate is in Switch mode. If the interface is a hardware switch, then your FortiGate is in Interface mode.

You can also determine what mode your FortiGate is by going to **System > Dashboard > Status** and enter either of the following commands into the **CLI Console**: `config system global show`. In the output that is displayed after you hit the Enter key, find the line that begins with `set internal-switch-mode`. This will tell you which mode your FortiGate is currently in.

If you need to change the mode your FortiGate unit is in, go to **System > Dashboard > Status** and enter either of the following commands into the **CLI Console**:

Before switching modes, you must make sure that none of the physical ports that make up the **lan** or **internal** interface are referenced in the FortiGate configuration.

1. Command to change the FortiGate to Switch mode:

```
config system global
   set internal-switch-mode switch
end
```

2. Command to change the FortiGate to Interface modeHub mode:

```
config system global
   set internal-switch-mode interface
end
```

There is a third mode, called Hub mode, that is available on some FortiGate models. Hub mode is similar to Switch mode, except the network device that it is emulating is a Layer 2 device instead of Layer 3. In Hub mode, he interfaces do not learn the MAC addresses of the devices on the network they are connected to and may also respond quicker to network changes in some circumstances.

You should only select Hub mode if you are having network performance issues when operating with Switch mode. The configuration of the FortiGate unit is the same whether in Switch mode or Hub mode.

Hardware Switches vs Software Switches

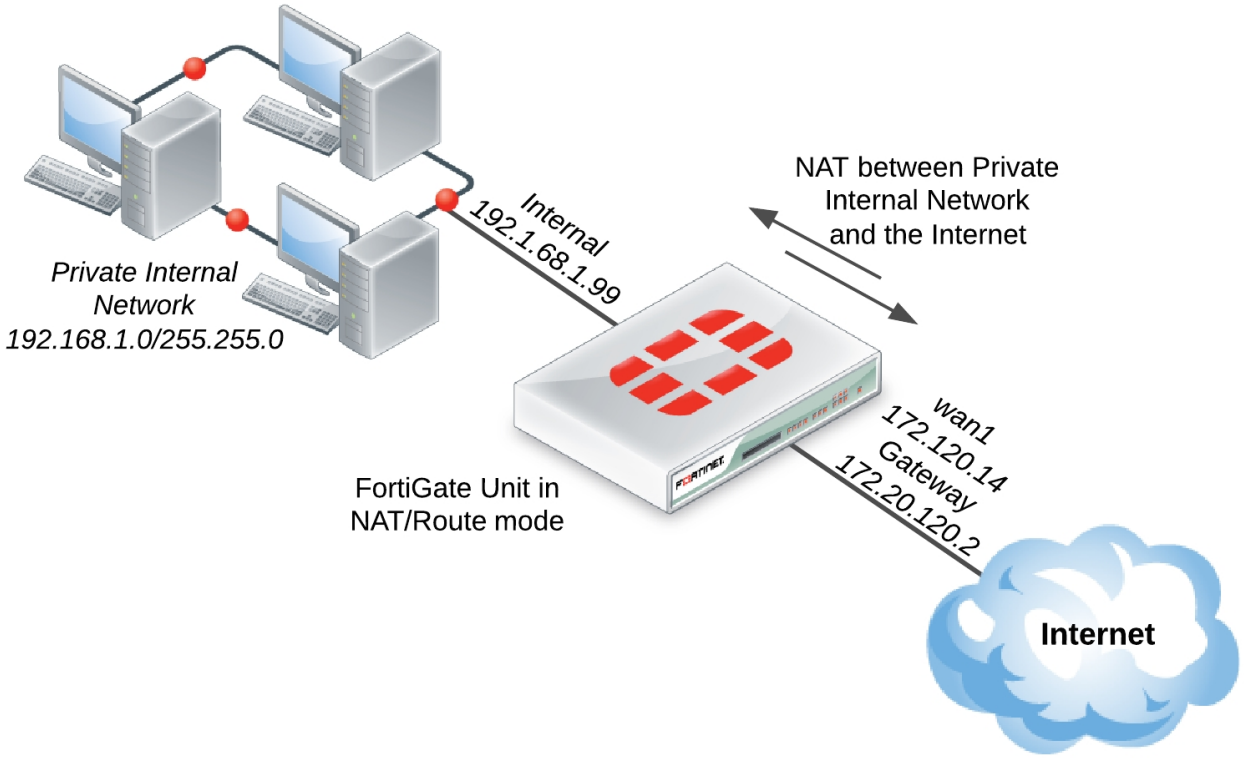
Both hardware and software switches are used to to allow ports to be grouped together and treated as a single interface. The main difference between the two types of switches is that hardware switches use the underlying switch chip/driver to handle all of the switching directly, while software switches do this in the FortiOS software.

The two types of switches also have differences in which commands and features are available, which vary depending on your FortiGate's model. In most situations, using a hardware switch is preferred for better performance, with software switches used in cases where a feature is required that is unavailable for a hardware switch.

For more information about creating hardware and software switches, please refer to the System Administration handbook.

Standard Installation in NAT/Route Mode

Network with a FortiGate unit in NAT/Route mode and a single ISP



1. Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment.
2. Connect a PC to the FortiGate using an internal port (typically port 1).
3. Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.
4. From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide). Login using an admin account (the default admin account has the username `admin` and no password).

5. Go to **System > Network > Interfaces** and edit the Internet-facing interface. Set **Addressing Mode** to **Manual** and the **IP/Netmask** to your public IP address. Select **OK**.
6. Edit the internal interface. Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate. Select **OK**.
7. Go to **Router > Static > Static Routes** (or **System > Network > Routing**, depending on your FortiGate model) and select **Create New** to add a default route. Set the **Destination IP/Mask** to 0.0.0.0/0.0.0.0, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements. Select **OK**.

A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can either edit it or delete it and add a new one.

8. (Optional) The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers. Select **Apply**.
9. If your network uses IPv4 addresses, go to **Policy & Objects > Policy > IPv4** and select **Create New** to add a security policy that allows users on the private network to access the Internet.

Some FortiGate models include the IPv4 security policy in the default configuration. If you have one of these models, this step has already been done for you and as soon as your FortiGate unit is connected and the computers on your internal network are configured, users should be able to access the Internet.

If your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Config > Features**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Handbook.

In the policy, set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to the Internet-facing interface. You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected. Select **OK**.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the Security Profiles handbook.

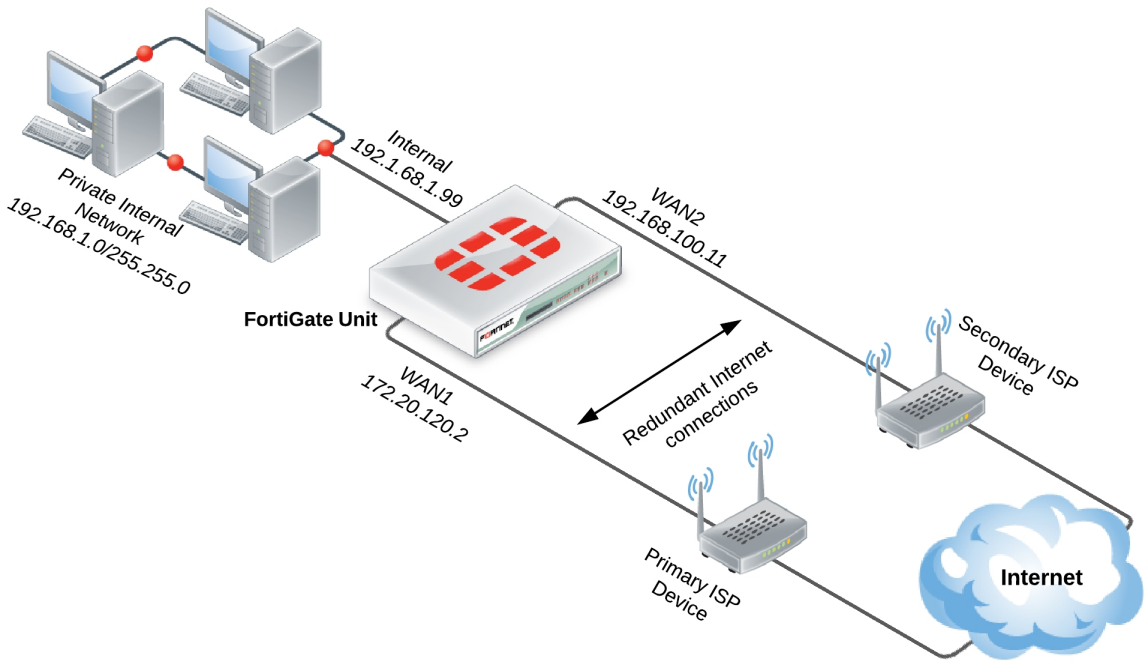
Results

Users on the internal network are now able to browse the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

Redundant Internet Installation in NAT/Route Mode

If you have previously configured your FortiGate using the standard installation, you will have to delete all routes and policies that refer to an interface that will be used to provide redundant Internet. This includes the default Internet access policy that is included on many FortiGate models.

Network with a FortiGate unit in NAT/Route mode using redundant Internet



1. Connect the FortiGate's Internet-facing interfaces (typically WAN1 and WAN2) to your ISP-supplied equipment.
2. Go to **System > Network > WAN Link Load Balancing** to create a WAN link interface, which is used to group multiple Internet connections together so that the FortiGate unit can treat them as a single interface.

If you are using FortiOS 5.2.0, go to **System > Network > Interfaces** and select **Create New > Virtual WAN** to create a virtual WAN link (this feature was renamed WAN link interface in FortiOS 5.2.1).

3. Select an appropriate method of **WAN Load Balancing** from the following options:

- **Source IP based -** The next hop is based on the traffic's source IP address.
- **Weighted Round Robin** - Weight is input for all the active members of the WAN link.
- **Spill-over** - A traffic cap is defined for active members; when it is exceeded, the traffic will automatically activate the standby link.
- **Source-Destination IP based** - The next hop is based on both the traffic's source and destination IP address.
- **Measured-Volume based -** A volume ratio is set for each active member of the WAN link.

4. Add your Internet-facing interfaces to the WAN link interface, configuring load balancing as required for each interface.
5. Go to **Router > Static > Static Routes** and create a new default route. Set **Device** to the virtual WAN link.
6. If your network uses IPv4 addresses, go to **Policy & Objects > Policy > IPv4** and select **Create New** to add a security policy that allows users on the private network to access the Internet.
   If your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Config > Features**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Handbook.
   In the policy, set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to the WAN link interface. You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.
7. Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected. Select **OK**.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the Security Profiles handbook.

Results

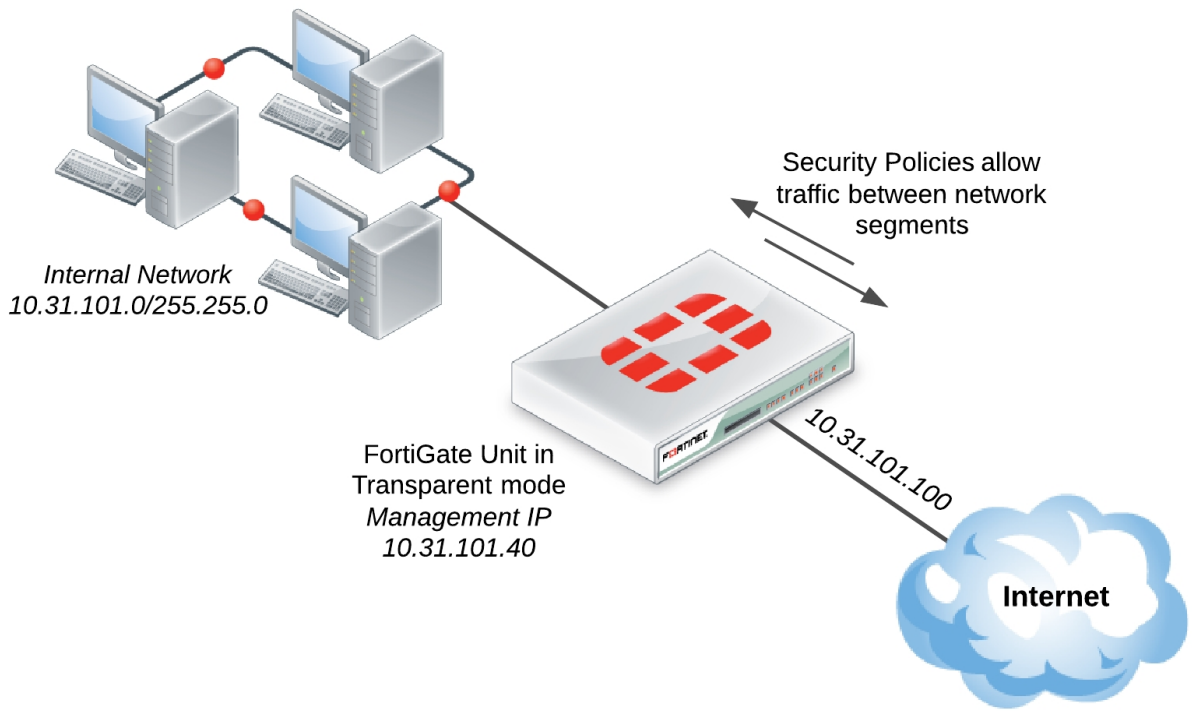
Users on the internal network are now able to browse the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

The amount of traffic will use an individual member of the WAN link interface will depend on the load balancing method you selected. You can view this usage by going to **System > FortiView > All Sessions** and viewing the **Dst Interface** column. If this column is not shown, right-click on the title row and select **Dst Interface** from the dropdown menu. Scroll to the bottom of the menu and select **Apply**.

Installing a FortiGate in Transparent Mode

Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

Network with a FortiGate unit in Transparent mode



1. Before connecting the FortiGate unit to your network, go to **System > Dashboard > Status** and locate the **System Information** widget. Beside **Operation Mode**, select **Change**.
2. Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network. Select **OK**.
3. Access the web-based manager by browsing to the new management IP.
4. (Optional) The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers. Select **Apply**.
5. If your network uses IPv4 addresses, go to **Policy & Objects > Policy > IPv4** and select **Create New** to add a security policy that allows users on the private network to access the Internet.
   If your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Config > Features**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Handbook.
   Set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to the Internet-facing interface (typically WAN1). You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.
6. Make sure the **Action** is set to **ACCEPT**. Select **OK**.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the Security Profiles handbook.

7. Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.
   Alternatively, you can also use the CLI command `execute shutdown`.
8. Connect the FortiGate unit between the internal network and the router.
9. Connect the Internet-facing interface to the router's internal interface and connect the internal network to the FortiGate using an internal port (typically port 1).
10. Power on the FortiGate unit. You will experience downtime before the FortiGate unit starts up completely.

Results

Users on the internal network are now able to browse to the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

If a FortiGate unit operating in Transparent mode is installed between your internet network and a server that is providing a network service to the internal network, such as DNS or DHCP, you must add a wan1-to-internal policy to allow the server's response to flow through the FortiGate unit and reach the internal network.

Troubleshooting your FortiGate Installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods (those methods that are only applicable to one transparent mode are marked):

1. **Use FortiExplorer if you can't connect to the FortiGate over Ethernet.**
   If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.
2. **Check for equipment issues.**
   Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.
3. **Check the physical network connections.**
   Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device.
   Also, check the **Unit Operation** widget, found at **System > Dashboard > Status**, to make sure the ports used in the connections are shown in green.
4. **Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).**
   Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.
   If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.
5. **Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).**
   From the internal network, attempt to ping the management IP address. If you cannot connect to the internal

interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

6. **Check the FortiGate interface configurations (NAT/Route mode).**
   Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure **Addressing Mode** is set to the correct mode.
7. **Verify the security policy configuration.**
   Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Sessions**, and select **Apply**).
   If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is turned on and that **Use Destination Interface Address** is selected.
8. **Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).**
   Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to Internet-facing interface.
9. **Verify the static routing configuration (NAT/Route mode).**
   Go to **Router > Static > Static Routes** or **System > Network > Routing** and verify that the default route is correct. View the Routing Monitor (found either on the same page or at **Router > Monitor > Routing Monitor**) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.
10. **Verify that you can connect to the gateway provided by your ISP.**
    Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.
11. **Verify that you can communicate from the FortiGate unit to the Internet.**
    Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.
12. **Verify the DNS configurations of the FortiGate unit and the PCs.**
    Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`
    If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.
13. **Confirm that the FortiGate unit can connect to the FortiGuard network.**
    Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, you should confirm that it can reach the FortiGuard network.
    First, check the **License Information** widget to make sure that the status of all FortiGuard services matches the services that you have purchased.
    Go to **System > Config > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the web-based manager should indicate a successful connection.
14. **Consider changing the MAC address of your external interface (NAT/Route mode).**
    Some ISPs do not want the MAC address of the device connecting to their network cable to change. If you have added a FortiGate unit to your network, you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
   edit <interface>
      set macaddr <xx:xx:xx:xx:xx:xx>
   end
```

```
end
```

15. Check the FortiGate bridge table (Transparent mode).
When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit.
Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed that is a likely cause. Check for the MAC address of the interface or device in question.
To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. This could indicate that the device is either not connected or not operating. Check the device's network connections and make sure they are connected and operational.

16. Either reset the FortiGate unit to factory defaults or contact the technical assistance center.
If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

You can also contact the technical assistance center. For contact information, go to support.fortinet.com.

Using Port Pairing to Simplify Transparent Mode

Once you have successfully installed a FortiGate in Transparent mode, you can use port pairing to simplify the configuration.

When you create a port pair, all traffic accepted by one of the paired interfaces can only exit out the other interface. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

Traffic between port-paired interfaces does not check the bridge table and MAC addresses are not learned. Instead traffic received by one interface in a port pair is forwarded out the other (if allowed by a firewall policy). This makes port pairing useful for unusual topologies where MAC addresses do not behave normally. For example, port paring can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

1. Go to *System* > *Network* > *Interfaces*. Select *Create New* > *Port Pair*. Create a port pair that includes both interfaces.
2. Go to *Policy & Objects* > *Policy* > *IPv4*. Create two security policy that allow traffic to flow between the interfaces in the port pair (for example, if you are pairing *wan1* and *Internal*, create a wan1-to-Internal policy and an Internal-to-wan1 policy).

Traffic should now be able to flow between the interfaces in the port pair. You can verify this by going to *Log & Report* > *Traffic Log* > *Forward Traffic*.

Using the Web-Based Manager

This section contains an introduction to the web-based manager administrative interface (sometimes referred to as a graphical user interface, or GUI) of your FortiGate unit and the information you can access from the various dashboards and tables.

The following topics are included in this section:

Connecting to the web-based manager
Menus
Dashboards
Feature settings
Information tables
Text strings

Connecting to the web-based manager

After you have completed the initial installation for your FortiGate unit, there are two ways to connect to the web-based manager: using FortiExplorer or a web browser.

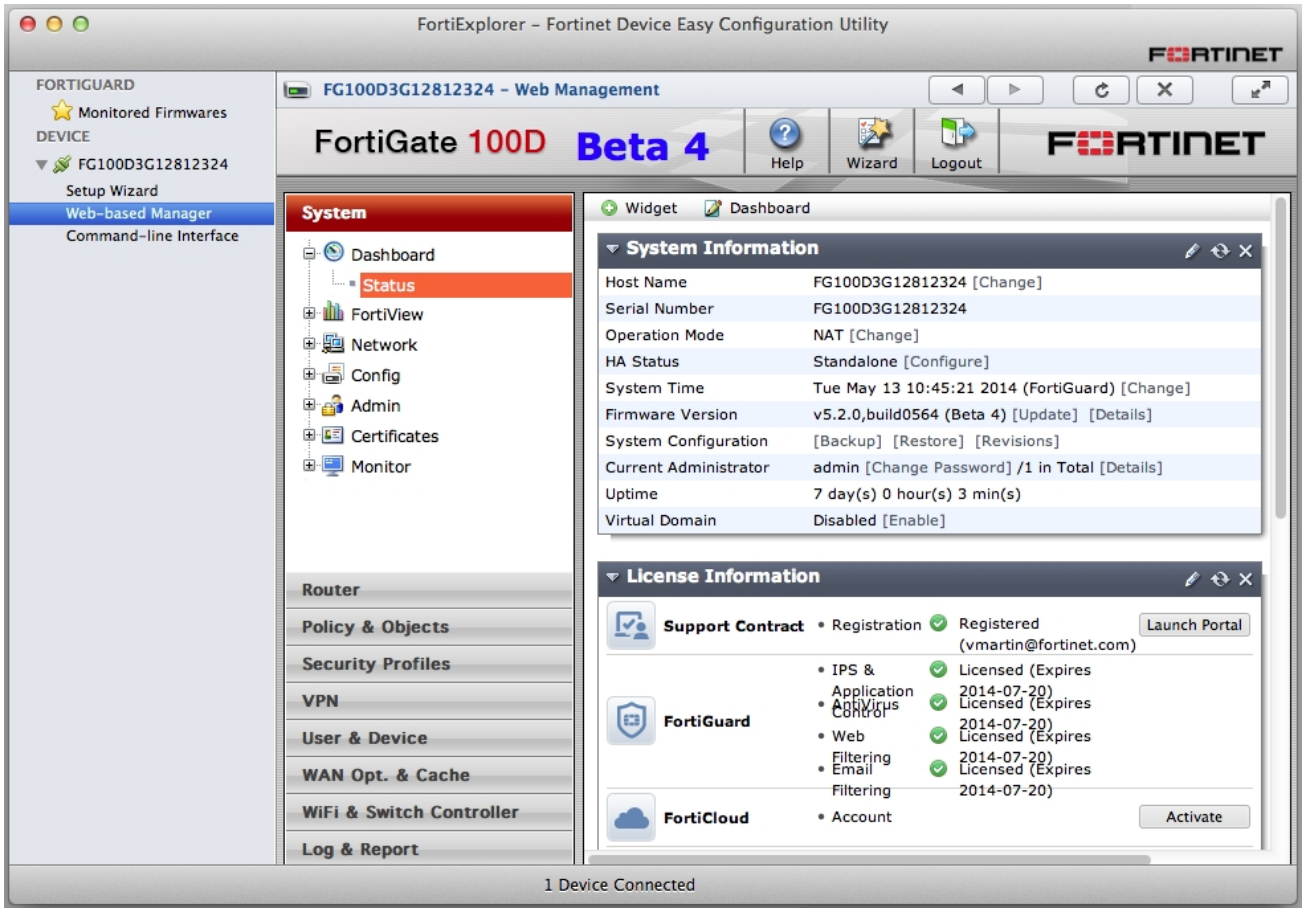
FortiExplorer

To connect to the web-based manager using FortiExplorer, connect your management computer to your FortiGate unit's USB MGMT port, using the cable that came with the unit. FortiExplorer should open automatically once the devices are connected; if it does not, open the program manually.

To connect to the web-based manager, go to **Devices > Web-based Manager** and enter your username and password. If you have not changed the admin account's password, use the default username, `admin`, and leave the password field blank.

The web-based manager will now be displayed in FortiExplorer.

Connecting to the web-based manager with FortiExplorer



Web browser

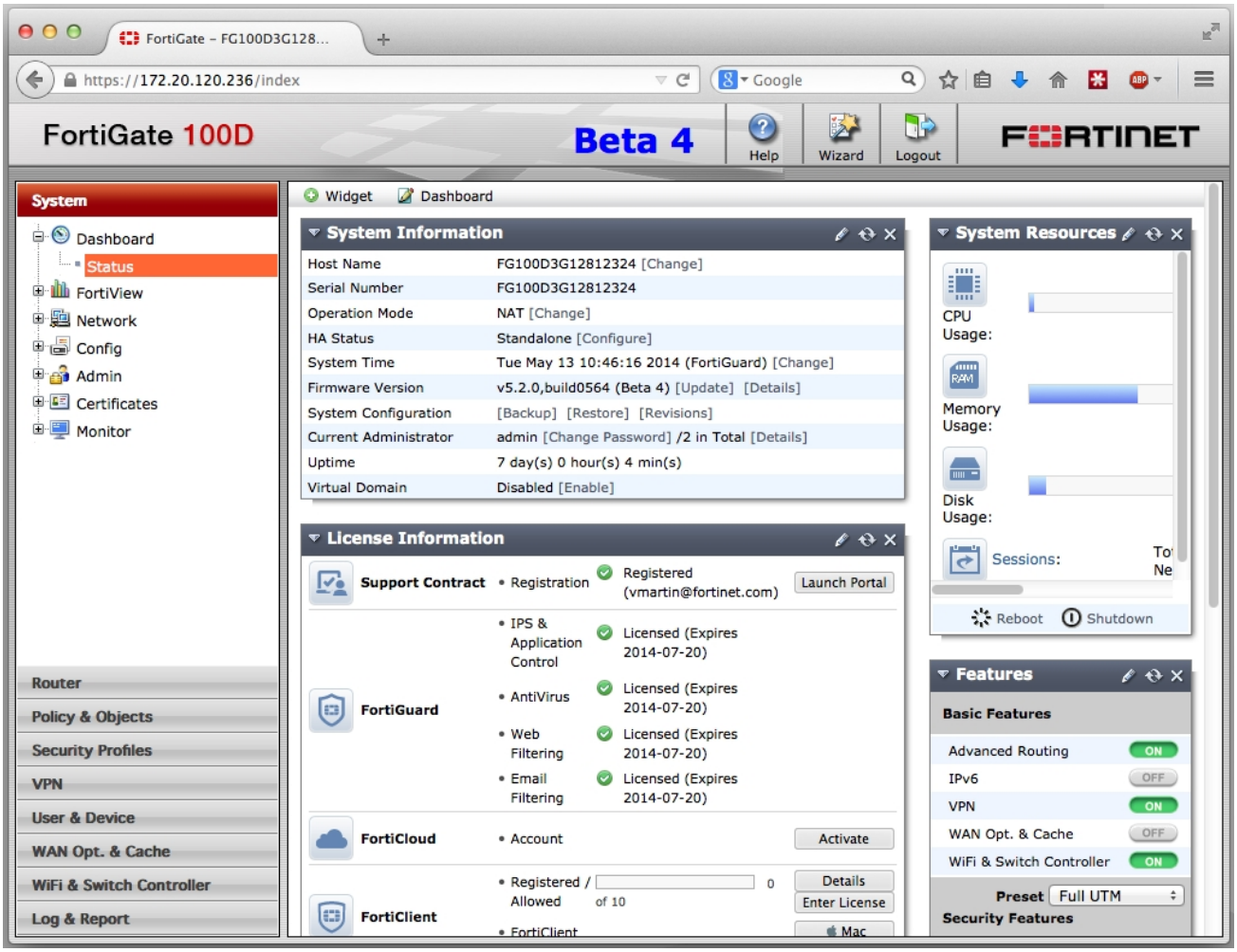
The recommended minimum screen resolution for properly displaying the web-based manager is 1280 by 1024. Check the FortiOS Release Notes for information about browser compatibility.

In order to connect to the web-based manager using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access, with the IP address 192.168.1.99.

Browse to https://192.168.1.99 and enter your username and password. If you have not changed the admin account's password, use the default username, `admin`, and leave the password field blank.

The web-based manager will now be displayed in your browser.

Connecting to the web-based manager with a web browser (Firefox)



If you wish to use a different interface to access the web-based manager, do the following:

1. Go to **System > Network > Interfaces** and edit the interface you wish to use for access. Take note of its assigned IP address.
2. Beside **Administrative Access**, select **HTTPS**. You can also select **HTTP**, although this is not recommended as the connection will be less secure.
3. Select **OK**.
4. Browse to the IP address using your chosen protocol.

The web-based manager will now be displayed in your browser.

Menus

Some menus may not initially appear on your FortiGate, while others only appear on certain FortiGate models or when certain features/modes are enabled. If there is a menu you believe your FortiGate model supports that does not appear in the web-based manager as expected, go to **System > Config > Features** and ensure the feature is turned on. For more information, see Feature settings on page 193.

The web-based manager contains the following main menus, which provide access to configuration options for most of the FortiOS features:

System	Configure system settings, such as network interfaces, virtual domains (VDOMs), DNS services, administrators, certificates, High Availability (HA), system time, set system options, and set display options on the web-based manager. The **System** menu also contains the Status and FortiView dashboards. For more information, see Dashboards on page 178 .
Router	Configure static, dynamic and multicast routing and view the router monitor. On certain FortiGate models, routing is configured by going to **System > Network > Routing**.
Policy & Objects	Configure firewall policies, protocol options, the Central NAT Table, and supporting content for policies including scheduling, services, traffic shapers, addresses, virtual IP and load balancing.
Security Profiles	Configure antivirus and email filtering, web filtering, intrusion protection, data leak prevention, application control, VOIP, ICAP and Client Reputation.
VPN	Configure IPsec and SSL virtual private networking.
User & Device	Configure user accounts and user authentication including external authentication servers.This menu also includes endpoint security features, such as FortiClient configuration and application detection patterns.
WAN Opt. & Cache	Configure WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers.
WiFi Controller	Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu is called **WiFi & Switch Controller** and has additional features allowing for FortiSwitch units to be managed by the FortiGate.
Log & Report	Configure logging and alert email as well as reports. View log messages and reports.
Current VDOM	This menu only appears when VDOMs are enabled on the unit and is used to switch between VDOMs.

Dashboards

The various dashboard menus provides a way to access information about network activity and events, as well as configure basic system settings.

There are two main dashboards: the Status Dashboard and the FortiView Dashboards.

Status Dashboard

The **Status Dashboard** can be found by going to **System > Dashboard > Status**. The dashboard consists of a number of widgets, each displaying a different set of information. A number of pre-configured widgets are available which can be customized to meet your needs.

To choose which widgets will be shown, select **Widget** and select the widget you wish to view, which will add it to the dashboard. Widgets can be rearranged in the **Status Dashboard** for easier access and viewing. You can also change the display from two columns to one by selecting the **Dashboard** button, selecting **Edit Dashboard** and choosing the one column display from the options.

Custom Dashboards

You can create custom dashboards that will be added to the menu under the default **Status Dashboard**. You can add, remove, or rename a dashboard, regardless of whether it is default. You can also reset the Dashboard menu to its default settings by selecting **Reset Dashboards**.

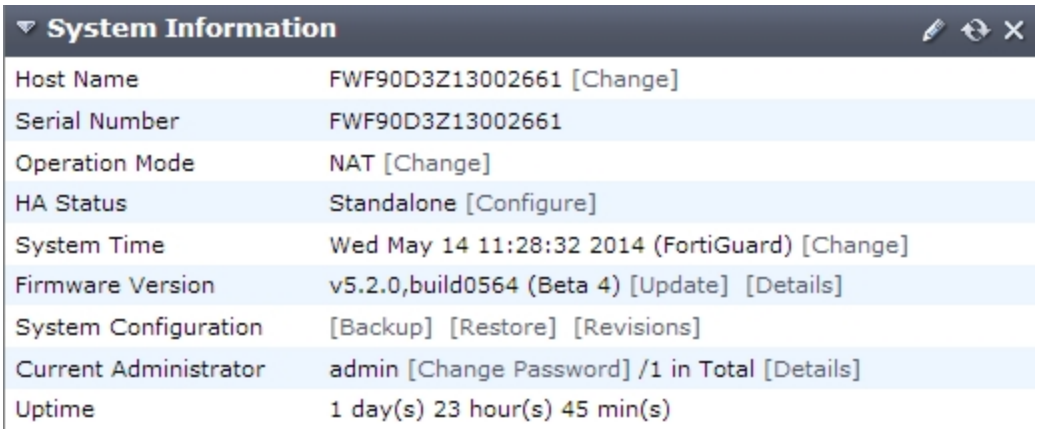
If VDOMs are enabled, only the dashboards within Global are available for configuration.

To add a dashboard

1. Go to **System > Dashboard > Status**.
2. Select **Dashboard**, located at the top left of the page.
3. Select **Add Dashboard**.

System Information

The System Information widget



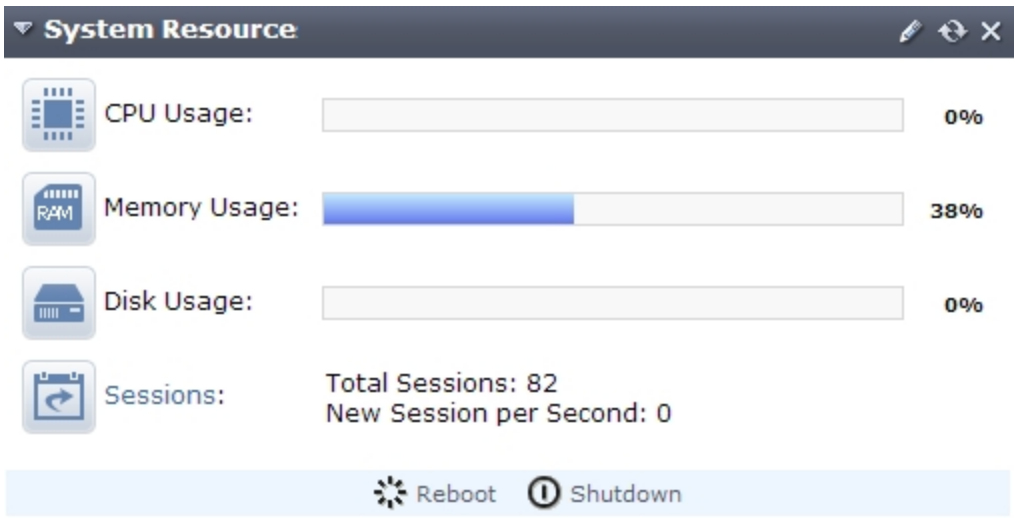
The **System Information** widget shows status information on the FortiGate unit. Some configuration details/modes can be changed through the widget.

Host Name	The name of the FortiGate unit. If the FortiGate unit is in HA mode, this information is not displayed.
Serial Number	The serial number of the FortiGate unit. The serial number is specific to that FortiGate unit and does not change with firmware upgrades.
Operation Mode	The current operating mode of the FortiGate unit (a FortiGate unit can operate in NAT mode or Transparent mode). If virtual domains are enabled, this field shows the operating mode of the current virtual domain. The Global System Status dashboard does not include this information.
HA Status	The status of High Availability (HA) within the cluster. Standalone indicates the FortiGate unit is not operating in HA mode. Active-Passive or Active-Active indicate the FortiGate unit is operating in HA mode. Select **Configure**, to change the HA configuration.
Cluster Name	The name of the HA cluster for this FortiGate unit. The FortiGate unit must be operating in HA mode to display this field.
Cluster Members	The FortiGate units in the HA cluster. Information displayed about each member includes host name, serial number, and whether the FortiGate unit is a primary (master) or subordinate (slave) FortiGate unit in the cluster. The FortiGate unit must be operating in HA mode with virtual domains disabled to display this information.
Virtual Cluster 1 **Virtual Cluster 2**	The role of each FortiGate unit in virtual cluster 1 and virtual cluster 2. The FortiGate unit must be operating in HA mode with virtual domains enabled to display this information.
System Time	The current date and time.
Firmware Version	The version of the current firmware installed on the FortiGate unit.
System Configuration	The time period of when the configuration file was backed up.
Current Administrator	The number of administrators currently logged into the FortiGate unit. Select **Details** to view more information about each administrator that is currently logged in
Uptime	The time in days, hours, and minutes since the FortiGate unit was started or rebooted.
Virtual Domain	Status of virtual domains on your FortiGate unit. This information will only appear when VDOMs have been enabled.

Explicit Proxy	The status of each feature. Select **Enable** or **Disable** to change the status of the feature. When enabled, the menu option appears.
Load Balance	This information will only appear when redundant Internet connections are enabled.

System Resources

The System Resources widget



The **System Resources** widget displays basic FortiGate unit resource usage. This widget displays the information for CPU and memory in either real-time or historical data. For FortiGate units with multiple CPUs, you can view the CPU usage as an average of all CPUs or each one individually.

This widget also is where you reboot or shutdown the FortiGate unit.

The options to reboot or shutdown the FortiGate unit are not available for an admin using the *prof_admin* profile.

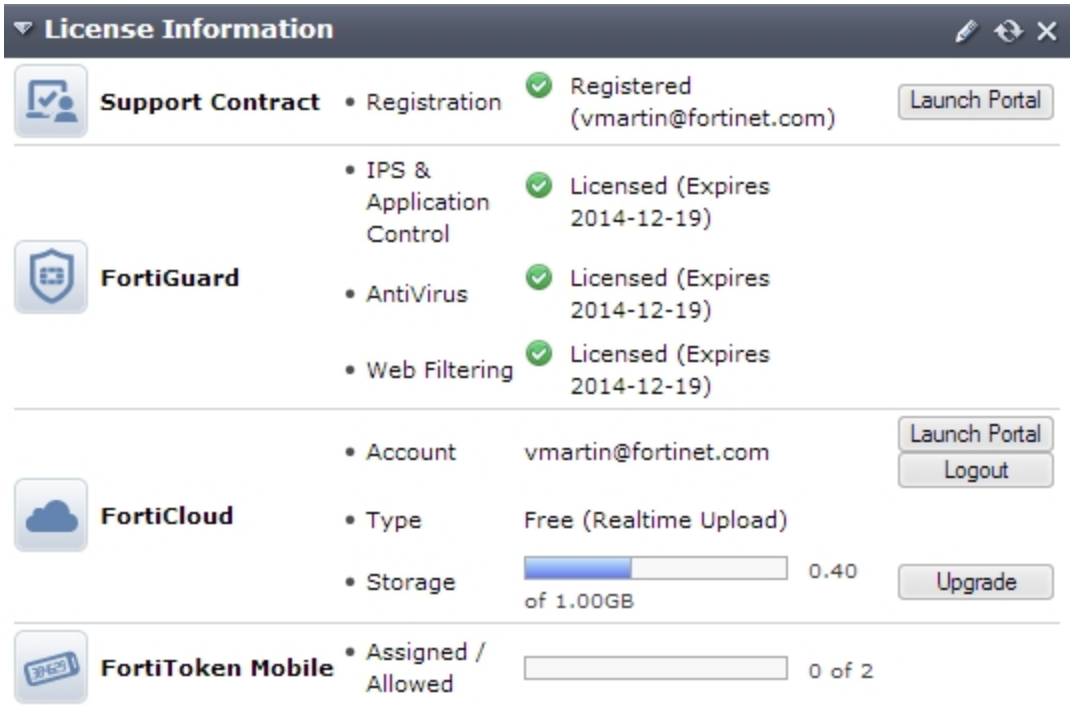
USB Modem

The USB modem widget

The USB modem widget enables you to monitor the status of your USB modem and configure it as needed.

License Information

The License Information widget



The **License Information** widget displays the status of your technical support contract, FortiGuard subscriptions, FortiCloud account, and other licenses.

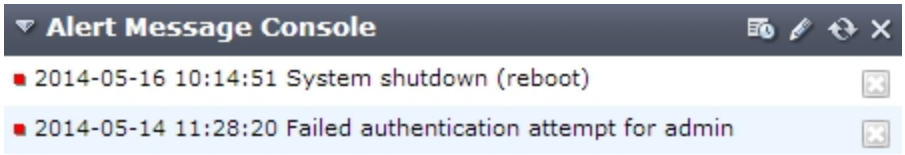
When a new FortiGate unit is powered on, it automatically searches for FortiGuard services. If the FortiGate unit is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The FortiGate unit sends its serial number to the FortiGuard service provider, which then determines whether the FortiGate unit is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the FortiGate unit is registered and has a valid contract, the **License Information** is updated.

When a license is near to its expiry date, an option to extend it will appear that allows you to add a new license as soon as you buy it.

Support Contract	Displays details about your current Fortinet Support contract. If **Not Registered** appears, select **Register** to register the FortiGate unit. If **Expired** appears, select **Renew** for information on renewing your technical support contract. Contact your local reseller. If **Registered** appears, the name of the support that registered this FortiGate unit is also displayed. The various types of contracts that you currently have and the expiry date for each type. You can select **Launch Portal** to log into the Fortinet Support account that registered this FortiGate unit.
FortiGuard Services	Displays your current licenses for services from FortiGuard. Select **Extend** or **Renew** to update any of the licenses (these options only appear when a license is expired or close to expiry).
FortiCloud	Displays details about your current FortiCloud subscription. If the green **Activate** button appears, select it to either create a new account or add the FortiGate unit to an existing account. If you have already activated FortiCloud, the name of the **Account** will be listed. Select **Launch Portal** to view your FortiCloud account in a web browser. Information on the current **Type** and **Storage** is also listed. You can select **Upgrade** to change the type of your FortiCloud account.
FortiClient Software	Displays FortiClient license details and the number of **Register** and **Allowed** FortiClient users. You can select **Details** for more information about the current FortiClient users. This information will only appear when you have a FortiClient license.
FortiToken Mobile	Displays the number of **Assigned** and **Allowed** FortiTokens.
SMS	Displays the number of **Sent** and **Allowed** SMS messages. You can select **Add Messages** to configure a new SMS message. This information will only appear when SMS has been configured.
Virtual Domain	Displays the maximum number of virtual domains the FortiGate unit supports with the current license. For some FortiGate models, you can select the **Purchase More** link to purchase a license key through Fortinet technical support to increase the maximum number of VDOMs.

Alert Message Console

The Alert Messages Console widget



The **Alert Messages Console** widget helps you monitor system events on your FortiGate unit such as firmware changes, network security events, or virus detection events. Each message shows the date and time that the event occurred.

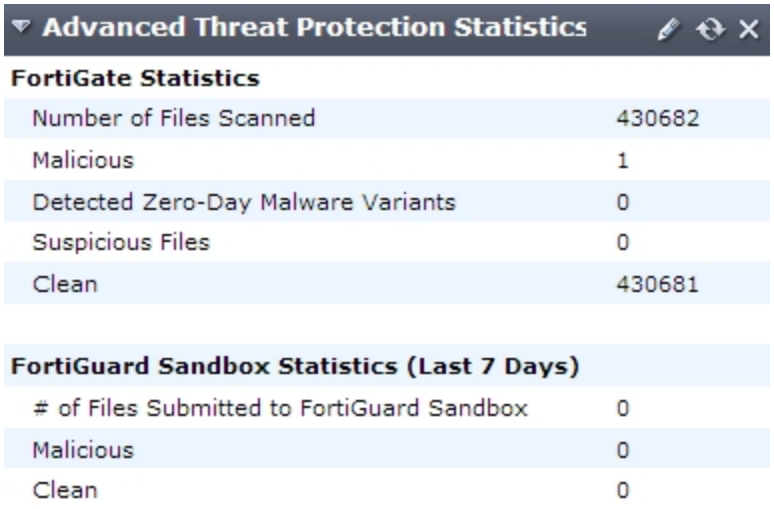
You can configure the alert message console settings to control what types of messages are displayed on the console.

To configure the Alert Message Console

1. Locate the **Alert Message Console** widget within the Dashboard menu.
2. Select the **Edit** icon in the **Alert Message Console** title bar.
3. Select the types of alerts that you do not want to be displayed in the widget.
4. Select **OK**.

Advanced Threat Protection Statistics

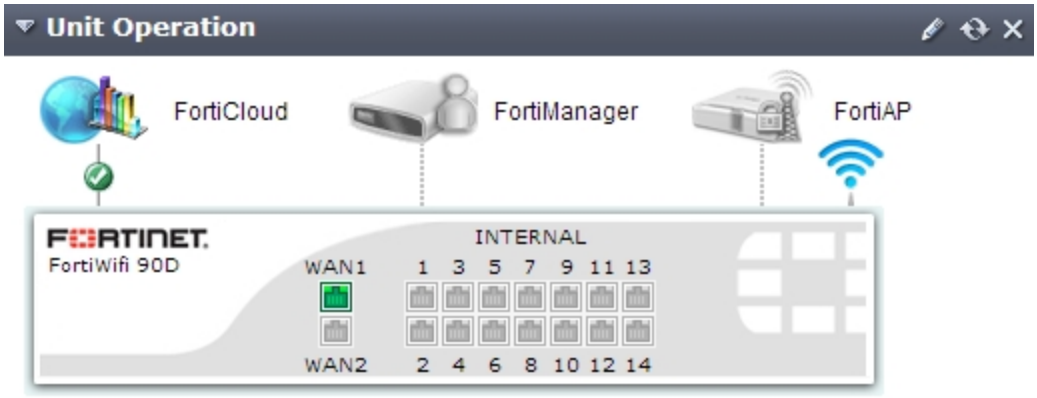
The Advanced Threat Protection Statistics widget



The **Advanced Threat Protection Statistics** widget displays a count of detected malware and files scanned for these types of intrusions. It also displays statics on the number of files sent to FortiGuard Sandbox and the results from sandboxing.

Unit Operation

The Unit Operation widget

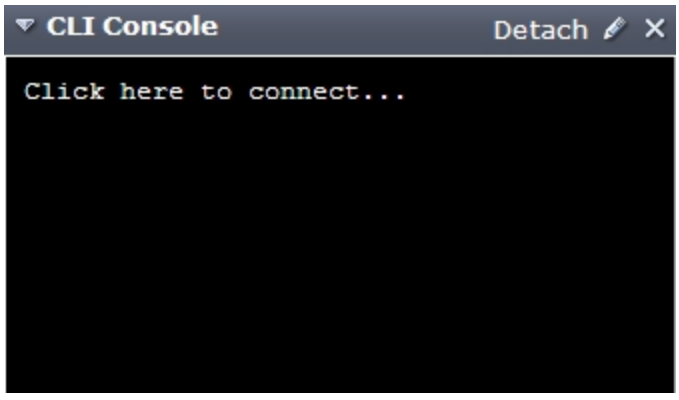


The **Unit Operation** widget is an illustrated version of the FortiGate unit's front panel that shows the status of the FortiGate unit's network interfaces. Interfaces appears green when connected. Hover the mouse pointer over an interface to view further details.

Icons around the front panel indicate when the FortiGate unit is connected to a FortiAnalyzer or FortiManager device, or FortiClient installations. Select the icon in the widget to jump to the configuration page for each device. When connected to one of these devices, a green check mark icon appears next to the icon. If the device communication is configured but the device is unreachable, a red X appears.

CLI Console

The CLI Console widget



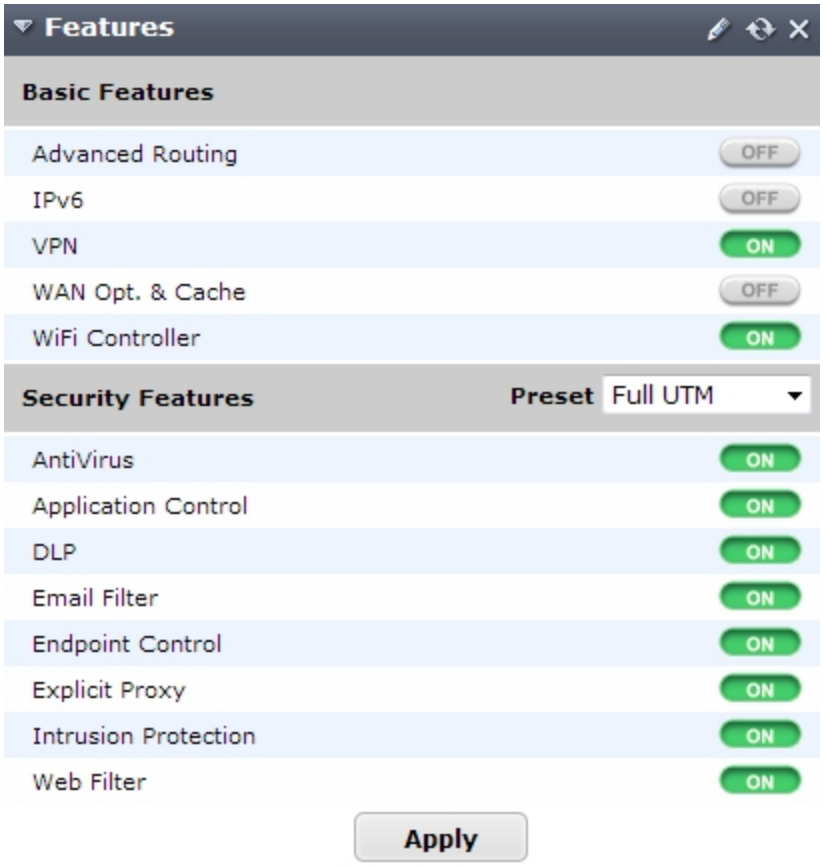
The **CLI Console** widget enables you to access the CLI without exiting from the web-based manager.

The two controls located on the CLI Console widget title bar are **Customize**, and **Detach**.

- **Detach** moves the CLI Console widget into a pop-up window that you can resize and reposition. Select **Attach**. to move the widget back to the dashboard's page.
- **Customize** enables you to change the appearance of the console by selecting fonts and colors for the text and background.

Features

The Features widget



The **Features** widget displays a number of **Basic Features** and **Security Features** and whether or not each feature is currently enabled or disabled. Options for features that are disabled will not appear in the web-based manager.

For more information, see Feature settings on page 193.

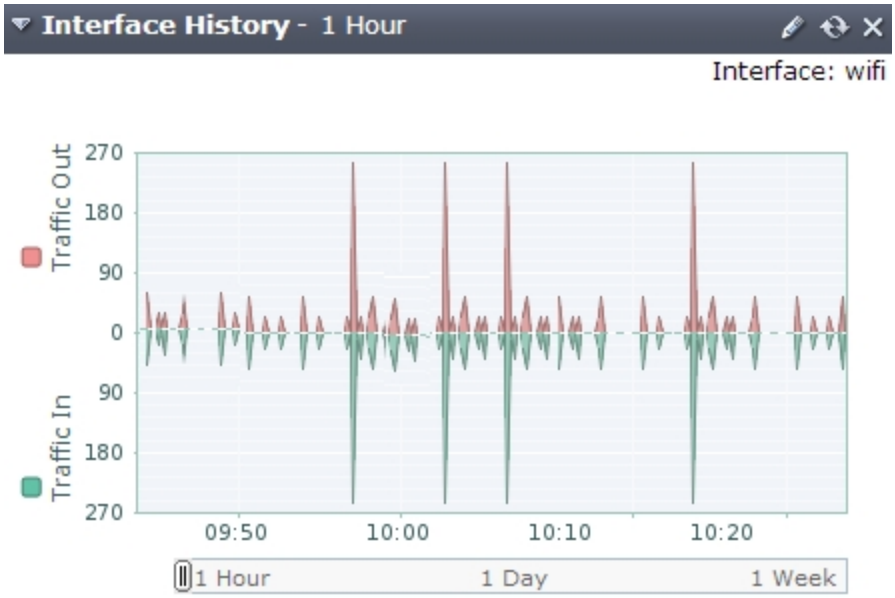
RAID monitor widget

The **RAID Monitor** widget displays the current state of the RAID array and each RAID disk. This widget does not display unless the FortiGate unit has more than one disk installed and is not available for FortiOS Carrier.

Array status icon	Displays the status of the RAID array. • Green with a check mark shows a healthy RAID array. • Yellow triangle shows the array is in a degraded state but it is still functioning. A degraded array is slower than a healthy array. Rebuild the array to fix the degraded state. • A wrench shows the array is being rebuilt. Positioning the mouse over the array status icon displays a text message of the status of the array.
Disk status icon	There is one icon for each disk in the array. • Green with a check mark shows a healthy disk. • Red with an X shows the disk has failed and needs attention. Positioning the mouse over the disk status icon displays the status of the disk, and the storage capacity of the disk.
RAID Level	The RAID level of this RAID array. The RAID level is set as part of configuring the RAID array.
Status bar	The bar shows the percentage of the RAID array that is currently in use.
Used/Free/Total	Displays the amount of RAID array storage that is being used, the amount of storage that is free, and the total storage in the RAID array. The values are in gigabytes.

Interface History

The Interface History widget

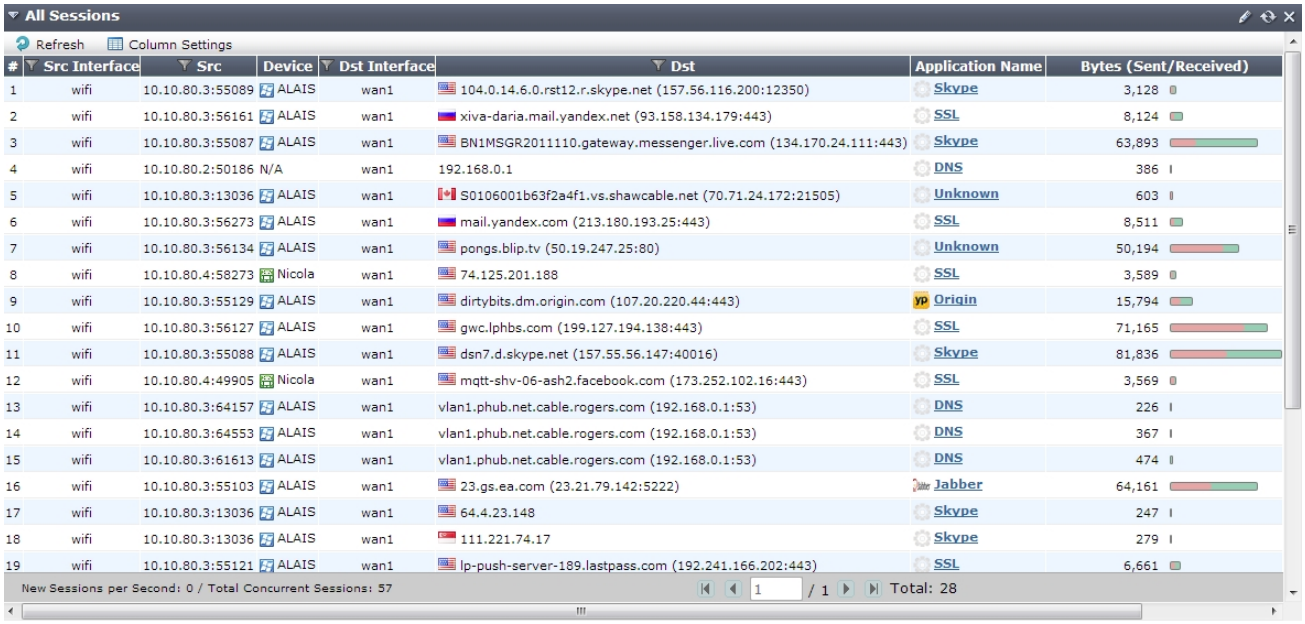


The **Interface History** widget displays the current activity and activity history of a system interface.

The current interface is visible in the top right-hand corner of the widget. You can change the interface that is shown by selecting the **Edit** icon and set **Select Network Interface** to the interface of your choice.

All Sessions

The All Sessions widget



The **All Sessions** widget shows information on your FortiGate's traffic. This widget can only be viewed on a dashboard that is set to have a one column display.

FortiView Dashboards

In order for information to appear in the **FortiView** dashboards, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Config > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

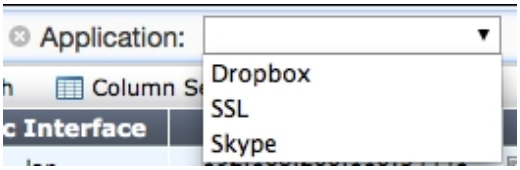
```
config log disk setting
     set status enable
end
```

Please note that flash-based logging has been disabled in FortiOS 5.2 for certain models. To view a complete list of affected models, please refer to the Release Notes.

The **FortiView** dashboards integrate real time and historical dashboards into a single view. These dashboards can be found by going to **Status > FortiView**. Each dashboard will initially display the top 100 sessions but when the results are filtered, other sessions may be displayed.

Each dashboards can be filtered by a variety of attributes. Attributes can be selected by using the dropdown menu located at the top of each widgets that displays only the options that have results; for example, if the only applications used in the are Dropbox, SSL, and Skype, the only options in the dropdown menu for the Application filter will be Dropbox, SSL, and Skype.

Filtering for Applications



Results can also be filtered using the various columns, although not all columns support this.

The dashboards also include different time options, allowing you to see current traffic in real-time, or historical traffic that occurred in the last 5 minutes, 1 hour, or 24 hours.

Historical traffic is only supported on FortiGate models that have local storage. The 24 hours option is also unavailable for desktop models (FortiGate-90 series and below).

Sources

The **Sources** dashboard shows information about the sources of traffic on your FortiGate unit, including user and device. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by source IP, source device, source interface, destination interface, and policy ID.

The Sources dashboard

Source	Device	Sessions	Bytes (Sent/Received)
10.10.80.3	Alais	122	539.94 K
10.10.80.4	Nicola	4	163.12 K
10.10.80.2	Wii	1	386

Applications

The **Applications** dashboard shows information about the applications being used on your network, including application name, category, and risk level. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the **Applications** dashboard, application control must be enabled in a policy.

The Applications dashboard

Application	Category	Risk	Sessions	Bytes (Sent/Received)
DNS	Network.Service		35	9.44 K
Skype	P2P		23	589.99 K
Hola.Unblocker	Proxy		21	440.08 K
SMTPS	Email		1	10.46 K
Dropbox	Storage.Backup		1	12.11 K

Cloud Applications

The **Cloud Applications** dashboard shows information about the cloud applications being used on your network, including application name, category, risk level, login IDs, and, if applicable, the number of videos played. If the cursor is held over the column showing the number of videos, the titles of these videos will be shown. Additional columns show information about sessions and bytes sent or received.

Two different views are available for the Cloud Applications dashboard: applications and users. Applications shows a list of the programs being used. Users shows information on the individual users of the cloud applications, including the username if the FortiGate was able to view the login event.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the **Cloud Applications** dashboard, an application control profile that has **Deep Inspection of Cloud Applications** turned on must be enabled in a policy and SSL Inspection must use `deep-inspection`.

Destinations

The **Destinations** dashboard shows information about the destination IPs of traffic on your FortiGate unit, as well as the application used. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by destination IP, user, source interface, destination interface, and policy ID.

The Destinations dashboard

Destination	Applicati...	Sessions	Bytes (Sent/Received)
pongs.blip.tv (54.243.171.49)	Unknown	2	71.42 K
gwb.lphbs.com (199.127.194.181)	Unknown	1	45.33 K
notify3.dropbox.com (108.160.167.157)	Dropbox	1	555
dsn0.d.skype.net (157.55.130.156)	Unknown	1	8.29 K
dsn15.d.skype.net (157.55.56.154)	Unknown	1	3.84 K
104.0.14.6.0.rst6.r.skype.net (157.55.133.145)	Unknown	1	5.03 K

Web Sites

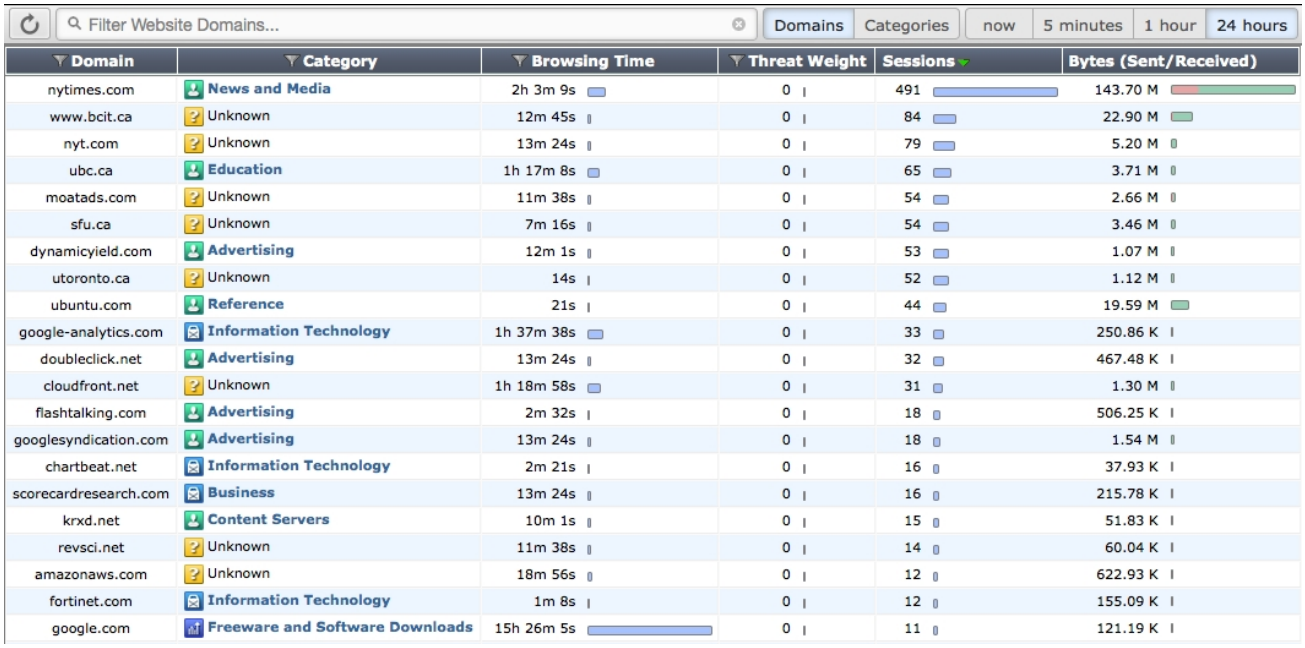
The **Web Sites** dashboard lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be clicked on in order to see a description of the category and several example sites, with content loaded from FortiGuard

on demand. New icons have also been added for FortiGuard category groups. Additional information is provided about domain, browsing time, threat weight, sources, and bytes sent or received.

This dashboard can be filtered by source interface, domain, destination interface, and policy ID.

In order for information to appear in the **Web Sites dashboard**, web filtering must be enabled in a policy, with FortiGuard Categories enabled.

The Web Sites dashboard



Domain	Category	Browsing Time	Threat Weight	Sessions	Bytes (Sent/Received)
nytimes.com	News and Media	2h 3m 9s	0	491	143.70 M
www.bcit.ca	Unknown	12m 45s	0	84	22.90 M
nyt.com	Unknown	13m 24s	0	79	5.20 M
ubc.ca	Education	1h 17m 8s	0	65	3.71 M
moatads.com	Unknown	11m 38s	0	54	2.66 M
sfu.ca	Unknown	7m 16s	0	54	3.46 M
dynamicyield.com	Advertising	12m 1s	0	53	1.07 M
utoronto.ca	Unknown	14s	0	52	1.12 M
ubuntu.com	Reference	21s	0	44	19.59 M
google-analytics.com	Information Technology	1h 37m 38s	0	33	250.86 K
doubleclick.net	Advertising	13m 24s	0	32	467.48 K
cloudfront.net	Unknown	1h 18m 58s	0	31	1.30 M
flashtalking.com	Advertising	2m 32s	0	18	506.25 K
googlesyndication.com	Advertising	13m 24s	0	18	1.54 M
chartbeat.net	Information Technology	2m 21s	0	16	37.93 K
scorecardresearch.com	Business	13m 24s	0	16	215.78 K
krxd.net	Content Servers	10m 1s	0	15	51.83 K
revsci.net	Unknown	11m 38s	0	14	60.04 K
amazonaws.com	Unknown	18m 56s	0	12	622.93 K
fortinet.com	Information Technology	1m 8s	0	12	155.09 K
google.com	Freeware and Software Downloads	15h 26m 5s	0	11	121.19 K

Threats

The **Threats** dashboard lists the top users involved in incidents, as well as information on the top threats to your network. Additional information is provided about the threat, category, threat level, threat weight, and number of incidents.

This dashboard can be filtered by source interface, threat type, threat, destination interface, and policy ID.

In order for information to appear in the **Threats** dashboard, **Threat Weight Tracking** must be used.

The Threats dashboard

Threat	Category	Threat Le...	Threat Weight	Incidents
Failed Connection Attempts	Failed Connection Attempts	Medium	30	3

All Sessions

The **All Sessions** dashboard shows information about all FortiGate traffic. To choose which columns you wish to view, select **Column Settings** and place your desired columns in the right-hand box, in the order that you wish them to appear.

This dashboard can be filtered by source IP, destination IP, application, source device, source interface, destination interface, and policy ID. If you have set a filter in a different dashboard before viewing the **All Sessions** dashboard, that filter will remain until manually cleared.

The All Sessions dashboard

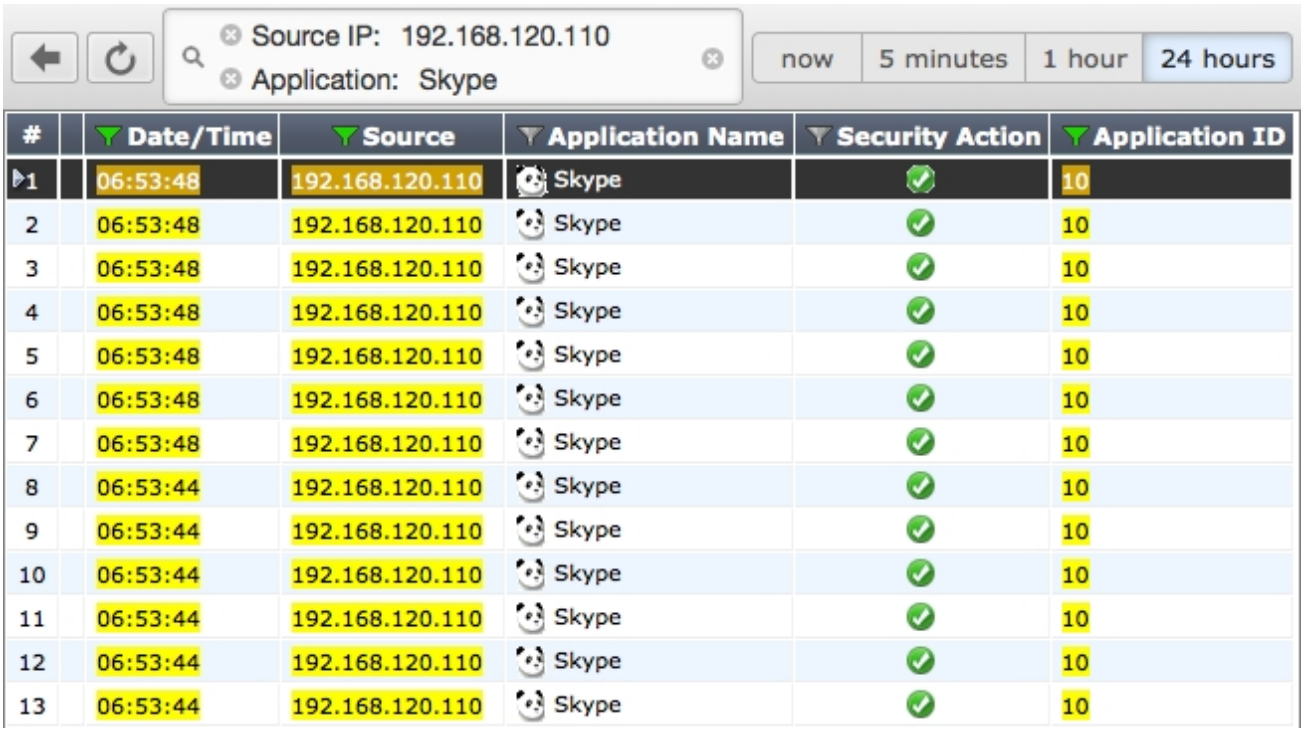
Date/Time	Source	Destination	Application Name	Security Acti...	Threat	Sent / Received
10:49:24	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown			4.11 KB / 11.33 KB
10:49:15	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown		AV EICAR_TEST_FILE	10.65 KB / 237.91 KB
10:44:33	192.168.120.110	38.127.167.7 (lastpass.com)	LastPass			2.02 KB / 8.98 KB
10:44:33	192.168.120.110	108.160.167.148 (d.dropbox.com)	Dropbox_Client.Sync			4.14 KB / 6.59 KB
10:44:26	192.168.120.110	134.170.24.141 (gateway.messenger.live.com)	Skype			10.75 KB / 33.54 KB
10:44:05	192.168.120.110	63.245.217.208 (phx-sync-13-2-8.services.mozilla.com)	SSL			8.66 KB / 4.39 KB

Drilldown Options

In all FortiView dashboards except for the **All Sessions** dashboard, you can view more information about a particular session by right-clicking or double-clicking on the session to display the **Drilldown to details...** option, which opens a summary page that includes further information about applications, sources, destinations, and sessions where applicable.

From this summary page, you can access automatically filtered logs that will show a list of applicable sessions. For example, if you have picked the IP address 192.168.120.110 from the **Sources** dashboard, you can then select **Drilldown to details...** for Skype from the **Applications** column. This will open a log that displays all sessions from 192.168.1.1 that used Skype. From this page, you can select **Drilldown to details...** for any individual session, in order to view the log entry for that session.

Viewing Skype sessions from the Source Address 192.168.120.110



#	Date/Time	Source	Application Name	Security Action	Application ID
1	06:53:48	192.168.120.110	Skype	✓	10
2	06:53:48	192.168.120.110	Skype	✓	10
3	06:53:48	192.168.120.110	Skype	✓	10
4	06:53:48	192.168.120.110	Skype	✓	10
5	06:53:48	192.168.120.110	Skype	✓	10
6	06:53:48	192.168.120.110	Skype	✓	10
7	06:53:48	192.168.120.110	Skype	✓	10
8	06:53:44	192.168.120.110	Skype	✓	10
9	06:53:44	192.168.120.110	Skype	✓	10
10	06:53:44	192.168.120.110	Skype	✓	10
11	06:53:44	192.168.120.110	Skype	✓	10
12	06:53:44	192.168.120.110	Skype	✓	10
13	06:53:44	192.168.120.110	Skype	✓	10

In the **All Sessions** dashboard, filters are also used to narrow down what results are shown. If you are viewing historical traffic in the **All Sessions** dashboard, you can also add an element to a filter by right-clicking the element and selecting **Set Filter**.

Feature settings

Feature settings are used to disable features which are not required for network administration. Disabling features also removes all related configuration options from the web-based manager.

Some features are disabled by default and must be enabled in order to configure them using the web-based manager.

Enabling/disabling features

Feature Settings can be selected using the **Features** widget on the Status page, found at **System > Dashboard > Status**. When viewed in the Status Dashboard, the **Features** widget only displays a limited number of features. To view the entire list, select the **Edit** option for the widget.

Feature Settings can also be found at **System > Config > Features**, where additional features are also available by selecting **Show More**.

Once you have accessed Feature Settings, ensure all features you wish to use are turned on, while features you wish to hide are turned off. When you have finished, select **Apply**.

Security Features Presets

The main Security Features can be turned off individually or the five system presets can be used:

- **Full UTM** should be chosen for networks that require full protection from FortiOS. UTM is the default setting.
- **WF** should be chosen for networks that require web filtering.
- **ATP** should be chosen for networks that require protection from viruses and other external threats.
- **NGFW** should be chosen for networks that require application control and protection from external attacks.
- **NGFW + ATP** should be chosen for networks that require protection from external threats and attacks.

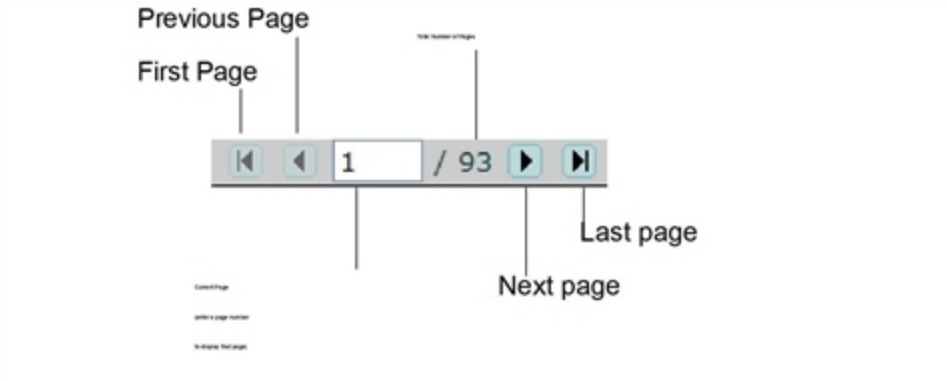
Information tables

Many of the web-based manager pages contain tables of information that you can filter to display specific information. Administrators with read and write access can define the filters.

Navigation

Some tables contain information and lists that span multiple pages. At the bottom of the page is the page navigation controls that enables you to move between pages.

Page controls



Adding filters to web-based manager lists

Filters are used to locate a specific set of information or content within multiple pages. These are especially useful in locating specific log entries. The specific filtering options vary, depending on the type of information in the log.

To create a filter, select **Filter Settings** or the filter icon in a column heading. When a filter is applied to a column, the filter icon becomes green. Filter settings are stored in the unit's configuration and will be maintained the next time that you access any list for which you have added filters.

Filtering variables can include: a numeric range (such as 25-50), an IP address or part of an address or any text string combination, including special characters.

Note that the filtering ignores characters following a "<" unless the followed by a space. For example, the filtering ignores `<string` but not `< string`. Filtering also ignores matched opening and closing (< and >) characters and any characters between them. For example, filtering will ignore `<string>`.

For columns that contain only specific content, such as log message severity, a list of terms is provided from which options can be selected.

Using column settings

Column settings are used to select the types of information which are displayed on a certain page. Some pages have a large amounts of information is available and not all content can be displayed on a single screen. Also, some pages may contain content that is not of use to you. Using column settings, you can display only that content which is important to your requirements.

To configure column settings, right-click the header of a column and select the columns you wish to view and de-select any you wish to hide. After you have finished making your selections, select **Apply** (you may need to scroll down the list to do so).

Any changes that you make to the column settings of a list are stored in the unit's configuration and will display the next time that you access the list. To return a page's columns to their default state, select **Reset All Columns**, located at the bottom of the **Column Settings** menu.

Text strings

The configuration of a FortiGate unit is stored in the FortiOS configuration database. To change the configuration, you can use the web-based manager or CLI to add, delete, or change configuration settings. These changes are stored in the database as you make them.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable) settings.

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

Most web-based manager text string fields make it easy to add an acceptable number of characters and prevent you from adding the XSS vulnerability characters.

There is a different character limitation for VDOM names and hostnames. For both, the only legal characters are numbers (0-9), letters (a-z, A-Z), and special characters - and _.

From the CLI, you can also use the `tree` command to view the number of characters that are allowed in a name field. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager, you are limited to entering 64 characters in the firewall address name field. From the CLI you can enter the following `tree` command to confirm that the firewall address `name` field allows 64 characters.

```
config firewall address
   tree
   -- [address] --*name (64)
   |- subnet
   |- type
   |- start-ip
   |- end-ip
   |- fqdn (256)
```

```
|- cache-ttl (0,86400)
|- wildcard
|- comment (64 xss)
|- associated-interface (16)
+- color (0,32)
```

The `tree` command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values set various sizes, rates, numeric addresses, and other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or, as in the case of MAC or IPv6 addresses, separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again, such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Basic Administration

This section contains information about basic FortiGate administration that can be done after you have installed the unit in your network.

While this section mainly focuses on tasks done using the web-based manager, some tasks include instructions to use the command line interface (CLI). You can connect to the CLI using the CLI widget, FortiExplorer, or by connecting using a SSH or Telnet connection. For more information about the CLI, see the System Administration handbook.

The following topics are included in this section:

Registration
System Settings
Firmware
FortiGuard
FortiCloud
Administrators
Passwords
Configuration Backups

Registration

In order to have full access to Fortinet Support and FortiGuard Services, you must register your FortiGate unit.

Registering your FortiGate:

1. Go to **System > Dashboard > Status** and locate the **License Information** widget.
2. Select **Register**.
3. In the pop-up window, either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.
4. Select **OK**.

System Settings

There are several system settings that should be configured once your FortiGate is installed.

Default administrator password

By default, your FortiGate has an administrator account set up with the username `admin` and no password. In order to prevent unauthorized access to the FortiGate, it is highly recommended that you add a password to this account.

To change the default password:

1. Go to **System > Admin > Administrators**.
2. Edit the **admin** account.
3. Select **Change Password**.

4. Leave **Old Password** blank, enter the **New Password** and re-enter the password for confirmation.
5. Select **OK**.

For details on selecting a password and password best practices, see Passwords on page 232.

Language

The default language of the web-based manager is English. To change the language, go to **System > Admin > Settings**. In the **Display Settings** section, select the language you want from the **Language** drop-down list. For best results, you should select the language that is used by the management computer.

Time and date

For effective scheduling and logging, the FortiGate system date and time should be accurate. You can either manually set the system date and time or configure the FortiGate unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

The Network Time Protocol enables you to keep the FortiGate time in sync with other network systems. By enabling NTP on the FortiGate unit, FortiOS will check with the NTP server you select at the configured intervals. This will also ensure that logs and other time-sensitive settings on the FortiGate unit are correct.

The FortiGate unit maintains its internal clock using a built-in battery. At startup, the time reported by the FortiGate unit will indicate the hardware clock time, which may not be accurate. When using NTP, the system time might change after the FortiGate has successfully obtained the time from a configured NTP server.

By default, FortiOS has the daylight savings time configuration enabled. The system time must be manually adjusted after daylight saving time ends. To disable DST, enter the following command in the CLI:

```
config system global
     set dst disable
end
```

To set the date and time

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Beside **System Time,** select **Change**.
3. Select your **Time Zone**.
4. Either select **Set Time** and manually set the system date and time, or select **Synchronize with NTP Server**. If you select synchronization, you can either use the default FortiGuard servers or specify a different server. You can also set the **Sync Interval**.
5. Select **OK**.

If you use an NTP server, you can identify a specific port/IP address for this self-originating traffic. The configuration is performed in the CLI with the command `set source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
   set ntpsyn enable
   set syncinterval 5
   set source-ip 192.168.4.5
end
```

Idle timeout

By default, the web-based manager disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the web-based manager if the management PC is left unattended.

To change the idle timeout

1. Go to **System > Admin > Settings**.
2. In the **Administration Settings** section, enter the time in minutes in the **Idle Timeout** field
3. Select **Apply**.

Administrator password retries and lockout time

By default, the FortiGate unit includes set number of three password retries, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this to further sway would-be hackers. Both settings are must be configured with the CLI

To configure the lockout options:

```
config system global
   set admin-lockout-threshold <failed_attempts>
   set admin-lockout-duration <seconds>
end
```

For example, to set the lockout threshold to one attempt and a five minute duration before the administrator can try again to log in enter the commands”

```
config system global
   set admin-lockout-threshold 1
   set admin-lockout-duration 300
end
```

Administrative port settings

In order to improve security, you can change the default port configurations for administrative connections to the FortiGate. When connecting to the FortiGate unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiGate unit using port 99, the url would be `https://192.168.1.99:99`.

To configure the lockout options:

1. Go to **System > Admin > Settings**.
2. Under **Administrative Settings,** change the port numbers for HTTP, HTTPS, Telnet, and/or SSH as needed. You can also select **Redirect to HTTPS** in order to avoid HTTP being used for the administrators.

When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique. If a conflict exists with a particular port, a warning message will appear.

Changing the host name

The host name of your FortiGate unit appears in the **Host Name** row, in the **System Information** widget. The host name also appears at the CLI prompt when you are logged in to the CLI and as the SNMP system name.

To change the host name on the FortiGate unit, in the **System Information** widget, select **Change** in the **Host Name** row. The only administrators that can change a FortiGate unit's host name are administrators whose admin profiles permit system configuration write access. If the FortiGate unit is part of an HA cluster, you should use a unique host name to distinguish the FortiGate unit from others in the cluster.

RAID disk configuration

The RAID disk is configured from the Disk Configuration page.

RAID level	Select the level of RAID. Options include: • **RAID-0** — (striping) better performance, no redundancy • **RAID-1** — (mirroring) half the storage capacity, with redundancy • **RAID-5** — striping with parity checking, and redundancy Available RAID level options depend on the available number of hard disks. Two or more disks are required for RAID 0 or RAID 1. Three or more disks are required for RAID 5. Changing the RAID level will erase any stored log information on the array, and reboot the FortiGate unit. The FortiGate unit will remain offline while it reconfigures the RAID array. When it reboots, the array will need to synchronize before being fully operational.
Status	The status, or health, of RAID array. This status can be one of: • **OK** — standard status, everything is normal. • **OK (Background-Synchronizing) (%)** — synchronizing the disks after changing RAID level, Synchronizing progress bar shows percent complete. • **Degraded** — One or more of the disks in the array has failed, been removed, or is not working properly. A warning is displayed about the lack of redundancy in this state. Also, a degraded array is slower than a healthy array. Select **Rebuild RAID** to fix the array. • **Degraded (Background-Rebuilding) (%)** — The same as degraded, but the RAID array is being rebuilt in the background. The array continues to be in a fragile state until the rebuilding is completed.
Size	The size of the RAID array in gigabytes (GB). The size of the array depends on the RAID level selected, and the number of disks in the array.
Rebuild RAID	Select to rebuild the array after a new disk has been added to the array, or after a disk has been swapped in for a failed disk. If you try to rebuild a RAID array with too few disks you will get a rebuild error. After inserting a functioning disk, the rebuild will start. This button is only available when the RAID array is in a degraded state and has enough disks to be rebuilt. You cannot restart a rebuild once a rebuild is already in progress. **Note:** If a disk has failed, the number of working disks may not be enough for the RAID level to function. In this case, replace the failed disk with a working disk to rebuild the RAID array.

Disk#	The disk's position in the array. This corresponds to the physical slot of the disk. If a disk is removed from the FortiGate unit, the disk is marked as not a member of the array and its position is retained until a new disk is inserted in that drive bay.
Status	The status of this disk. Options include OK, and unavailable. A disk is unavailable if it is removed or has failed.

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the Release Notes for a new firmware release.
- Review the Supported Upgrade Paths document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration, including local certificates. For more information, see Configuration Backups on page 233.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Backing up the current configuration

In case you need to restore your FortiGate configuration, you should always back up the configuration before installing new firmware.

To create a local backup:

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Select **Backup** beside **System Configuration**.
3. Choose either **Local PC** or **USB Disk** to save the configuration file.
4. If desired, select **Encrypt configuration file**.
5. Select **Backup**.

Downloading firmware

Firmware images for all FortiGate units is available on the Fortinet Customer Support website, https://support.fortinet.com.

To download firmware

1. Log into the site using your user name and password.
2. Go to **Download > Firmware Images**.
3. A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware you wish to upgrade your FortiGate unit to.
4. Select **HTTPS Download**.

Firmware can also be downloaded using FTP; however, as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

5. Navigate to find the folder for the firmware version you wish to use.
6. Select your FortiGate model from the list. If your unit is a FortiWiFi, be sure to get the appropriate firmware, which will have a filename starting with FWF.
7. Save the firmware image to your computer.

Testing new firmware before installing

FortiOS enables you to test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure Upgrading the firmware - web-based manager on page 205 .

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 or null modem cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure, you must install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Enter the following command to restart the FortiGate unit:

```
execute reboot
```

6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages appears.
   When the following messages appears:

```
Press any key to display configuration menu....
```

7. Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must login and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
    [H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press **Enter**.

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address of the FortiGate unit to connect to the TFTP server.

    The IP address must be on the same network as the TFTP server.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image file name and press **Enter**.

    The TFTP server uploads the firmware image file to the FortiGate unit and the following appears.

    ```
    Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
    ```

12. Type `R`.

    The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

You can test the new firmware image as required. When done testing, you can reboot the FortiGate unit, and the FortiGate unit will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware - web-based manager

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware

1. Log into the web-based manager as the admin administrative user.
2. Go to **System > Dashboard > Status** and locate the **System Information** widget.
3. Beside **Firmware Version**, select **Update**.
4. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
5. Select **OK**.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

Upgrading the firmware - CLI

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For more information, see the System Administration handbook.

Before you begin, ensure you have a TFTP server running and accessible to the FortiGate unit.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware using the CLI

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of

the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image.out 192.168.1.168
```

The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
    Do you want to continue? (y/n)
```

6. Type `y`.
7. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
8. Reconnect to the CLI.
9. Update antivirus and attack definitions, by entering:

```
execute update-now
```

Installing firmware from a system reboot using the CLI

There is a possibility that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots. If this occurs, it is best to perform a fresh install of the firmware from a reboot using the CLI.

This procedure installs a firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9, or null modem cable. This procedure reverts the FortiGate unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the FortiGate unit configuration.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

6. Enter the following command to restart the FortiGate unit.

```
execute reboot
```

The FortiGate unit responds with the following message:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

7. Type `y`.

As the FortiGate unit starts, a series of system startup messages appears. When the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get to the new firmware image form the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

9. Type the address of the TFTP server and press **Enter**.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

10. Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image filename and press **Enter**.

The TFTP server uploads the firmware image file to the FortiGate unit and a message similar to the following appears:

```
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
```

12. Type `D`.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Reverting to a previous firmware version - web-based manager

The following procedures revert the FortiGate unit to its factory default configuration and deletes any configuration settings. If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Always remember to back up your configuration before making any changes to the firmware.

To revert to a previous firmware version

1. Go to **System > Dashboard > Status** and locate the **System Information widget**.
2. Beside **Firmware Version**, select **Update**.
3. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
4. Select **OK**.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

Reverting to a previous firmware version - CLI

This procedure reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

To use the following procedure, you must have a TFTP server the FortiGate unit can connect to.

To revert to a previous firmware version using the CLI

1. Make sure the TFTP server is running
2. Copy the firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI.
4. Make sure the FortiGate unit can connect to the TFTP server execute by using the `execute ping` command.
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image28.out 192.168.1.168
   ```

   The FortiGate unit responds with this message:

```
This operation will replace the current firmware version!
    Do you want to continue? (y/n)
```

6. Type `y`.

   The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```

7. Type `y`.
8. The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
9. Reconnect to the CLI.
10. To restore your previous configuration, if needed, use the command:

    ```
    execute restore config <name_str> <tftp_ip4>
    ```

11. Update antivirus and attack definitions using the command:

    ```
    execute update-now.
    ```

Restore from a USB key - CLI

To restore configuration using the CLI

1. Log into the CLI.
2. Enter the following command to restore an unencrypted configuration file:

   ```
   exec restore image usb <filename>
   ```

   If your configuration file was encrypted, enter the following command:

   ```
   execute restore config usb-mode <password>
   ```

   The FortiGate unit responds with the following message:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```

3. Type `y`.

Configuration revision

The **Configuration Revisions** menu enables you to manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive. The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed in the **System Information** widget on the Dashboard.

Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can also be configured so that when it is rebooted, it will automatically load the new firmware (CLI only). Using this option, you can stage a number of FortiGate units to do an upgrade simultaneously to all devices using FortiManager or script.

To load the firmware for later installation - web-based manager

1. Go to **System > Dashboard > Status**.
2. Under **System Information > Firmware Version**, select **Update**.
3. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
4. Deselect the **Boot the New Firmware** option.
5. Select **OK**.

To load the firmware for later installation - CLI

```
execute restore secondary-image {ftp | tftp | usb}
```

To set the FortiGate unit so that when it reboots, the new firmware is loaded, use the CLI command…

```
execute set-next-reboot {primary | secondary}
```

… where `{primary | secondary}` is the partition with the preloaded firmware.

To trigger the upgrade using the web-based manager

1. Go to **System > Dashboard > Status**.
2. Under **System Information > Firmware Version**, select **Details**.
3. Select the check box for the new firmware version.
   The **Comments** column indicates which firmware version is the current active version.
4. Select **Upgrade** icon.

FortiGuard

The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.

The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats.The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.

The FortiGuard services provide a number of services to monitor world-wide activity and provide the best possible security:

- **Intrusion Prevention** System (IPS)- The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been

developed. It also provides more than 1000 application identity signatures for complete application control.

- **Application Control** - Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.
- **AntiVirus** -The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.
- **Web Filtering** - Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages - all continuously updated.
- **Vulnerability Scanning** - FortiGuard Services provide comprehensive and continuous updates for vulnerabilities, remediation, patch scan, and configuration benchmarks.
- **Email Filtering** - The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously via the FDN.
- **Messaging Services** - Messaging Services allow a secure email server to be automatically enabled on your FortiGate unit to send alert email or send email authentication tokens. With the SMS gateway, you can enter phone numbers where the FortiGate unit will send the SMS messages. Note that depending on your carrier, there may be a slight time delay on receiving messages.
- **DNS and DDNS** - The FortiGuard DNS and DDNS services provide an efficient method of DNS lookups once subscribed to the FortiGuard network. This is the default option. The FortiGate unit connects automatically to the FortiGuard DNS server. If you do not register, you need to configure an alternate DNS server.

  Configure the DDNS server settings using the CLI commands:

```
config system fortiguard
   set ddns-server-ip
   set ddns-server-port
end
```

Support Contract and FortiGuard Subscription Services

The **Support Contract** and **FortiGuard Subscription Services** sections are displayed in abbreviated form within the **License Information** widget. A detailed version is available by going to **System > Config > FortiGuard**.

The Support Contract area displays the availability or status of your FortiGate unit's support contract. The status displays can be either **Unreachable, Not Registered,** or **Valid Contract**.

The FortiGuard Subscription Services area displays detailed information about your FortiGate unit's support contract and FortiGuard subscription services. On this page, you can also manually update the antivirus and IPS engines.

The status icons for each section Indicates the state of the subscription service. The icon corresponds to the availability description.

- **Gray (Unreachable)** – the FortiGate unit is not able to connect to service.
- **Orange (Not Registered)** – the FortiGate unit can connect, but not subscribed.
- **Yellow (Expired)** – the FortiGate unit had a valid license that has expired.

- **Green (Valid license)** – the FortiGate unit can connect to FDN and has a registered support contract. If the Status icon is green, the expiry date also appears.

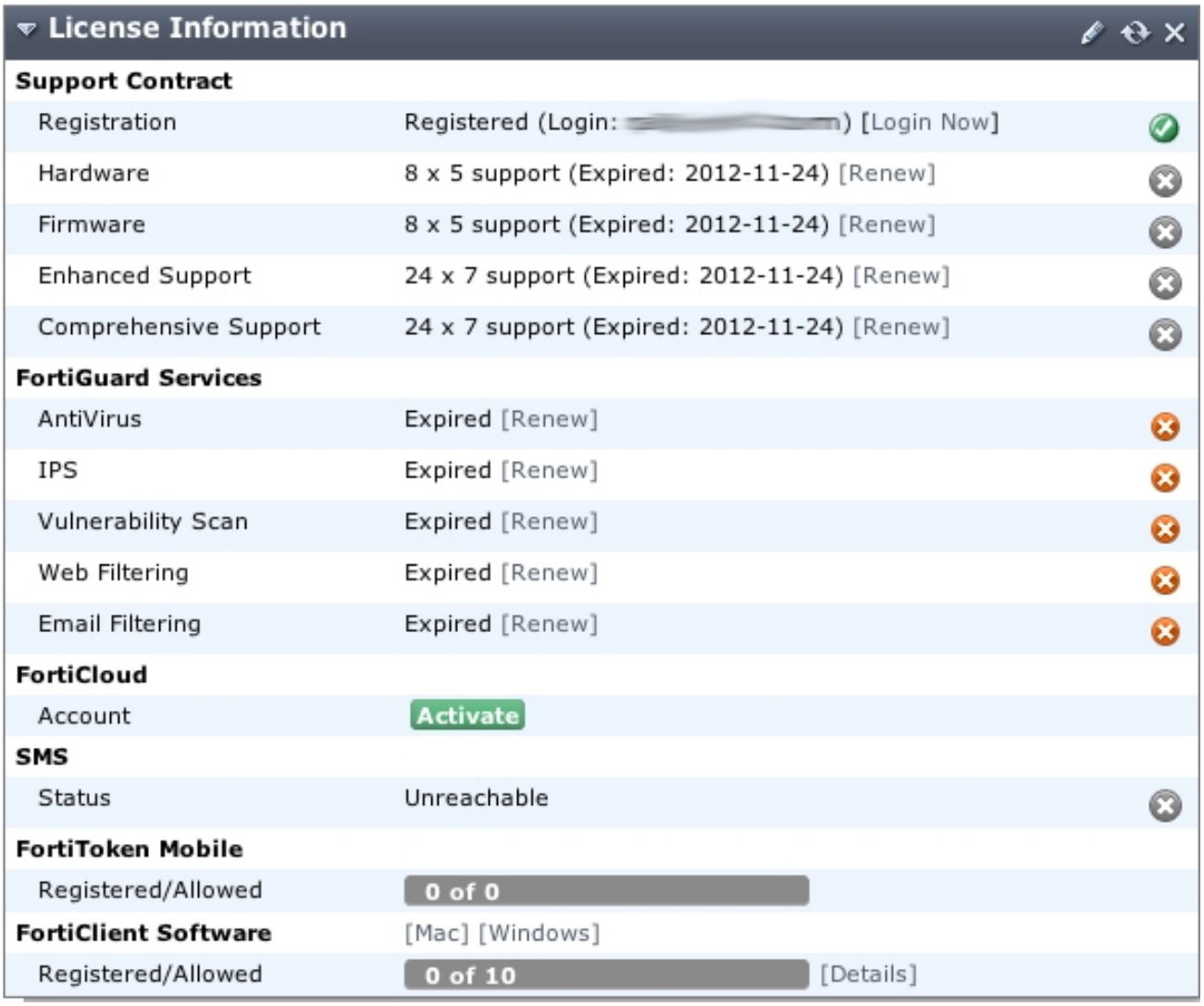
Verifying your Connection to FortiGuard

If you are not getting FortiGuard web filtering or antispam services, there are a few things to verify communication to the FortiGuard Distribution Network (FDN) is working. Before any troubleshooting, ensure that the FortiGate unit has been registered and you or your company, has subscribed to the FortiGuard services.

Verification - web-based manager

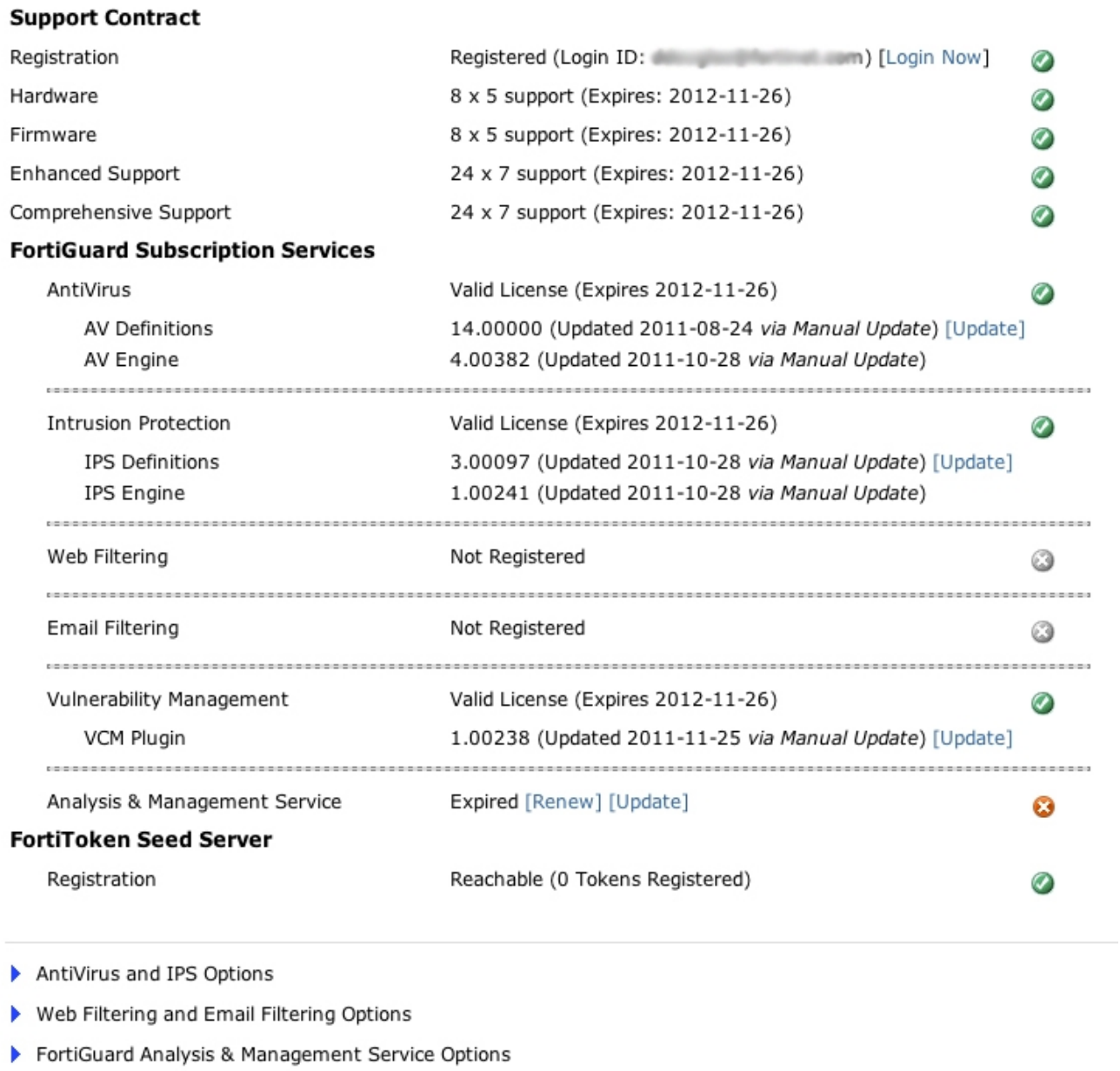
The simplest method to check that the FortiGate unit is communicating with the FDN, is to check the **License Information** dashboard widget. Any subscribed services should have a green check mark beside them indicating that connections are successful. Any other icon indicates a problem with the connection, or you are not subscribed to the FortiGuard services.

License Information widget showing FortiGuard availability



You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.

FortiGuard availability



Verification - CLI

You can also use the CLI to see what FortiGuard servers are available to your FortiGate unit. Use the following CLI command to ping the FDN for a connection:

```
ping guard.fortinet.net
```

You can also use diagnose command to find out what FortiGuard servers are available:

```
diagnose debug rating
```

From this command, you will see output similar to the following:

```
Locale : english
License : Contract
Expiration : Sun Jul 24 20:00:00 2011
Hostname : service.fortiguard.net
-=- Server List (Tue Nov 2 11:12:28 2010) -=-

IP Weight      RTT Flags  TZ   Packets   Curr Lost   Total Lost
69.20.236.180  0   10     -5   77200 0           42
69.20.236.179  0   12     -5   52514     0           34
66.117.56.42   0   32     -5   34390     0 62
80.85.69.38    50  164     0   34430     0           11763
208.91.112.194 81  223 D  -8   42530     0           8129
216.156.209.26 286 241 DI -8   55602     0          21555
```

An extensive list of servers are available. Should you see a list of three to five available servers, the FortiGuard servers are responding to DNS replies to service.FortiGuard.net, but the INIT requests are not reaching FDS services on the servers.

The rating flags indicate the server status:

D	Indicates the server was found via the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with 'D' and will be used first for INIT requests before falling back to the other servers.
I	Indicates the server to which the last INIT request was sent
F	The server has not responded to requests and is considered to have failed.
T	The server is currently being timed.

The server list is sorted first by weight and then the server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost, it will be resent to the next server in the list.

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a faraway server, the weight is not allowed to dip below a base weight, which is calculated as the difference in hours between the FortiGate unit and the server multiplied by 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Port assignment

FortiGate units contact the FortiGuard Distribution Network (FDN) for the latest list of FDN servers by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets have a destination port of 1027 or 1031.

If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets. As a result, the FortiGate unit will not receive the complete FDN server list.

If your ISP blocks the lower range of UDP ports (around 1024), you can configure your FortiGate unit to use higher-numbered ports, using the CLI command…

```
config system global
   set ip-src-port-range <start port>-<end port>
```

```
end
```

…where the <start port> and <end port> are numbers ranging of 1024 to 25000.

For example, you could configure the FortiGate unit to not use ports lower than 2048 or ports higher than the following range:

```
config system global
   set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use. Push updates might be unavailable if:

- there is a NAT device installed between the unit and the FDN
- your unit connects to the Internet using a proxy server.

FortiCloud is a hosted security management and log retention service for FortiGate products. It gives you a centralized reporting, traffic analysis, configuration and log retention without the need for additional hardware and software.

Configuring Antivirus and IPS Options

Go to **System > Config > FortiGuard**, and expand the **AV and IPS Options** section to configure the antivirus and IPS options for connecting and downloading definition files.

Use override server address	Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.
Allow Push Update	Select to allow updates sent automatically to your FortiGate unit when they are available
Allow Push Update status icon	The status of the FortiGate unit for receiving push updates: • **Gray (Unreachable)** - the FortiGate unit is not able to connect to push update service • **Yellow (Not Available)** - the push update service is not available with your current support license • **Green (Available)** - the push update service is allowed.
Use override push IP and Port	Available only if both **Use override server address** and **Allow Push Update** are enabled. Enter the IP address and port of the NAT device in front of your FortiGate unit. FDS will connect to this device when attempting to reach the FortiGate unit. The NAT device must be configured to forward the FDS traffic to the FortiGate unit on UDP port 9443.
Schedule Updates	Select this check box to enable updates to be sent to your FortiGate unit at a specific time. For example, to minimize traffic lag times, you can schedule the update to occur on weekends or after work hours. Note that a schedule of once a week means any urgent updates will not be pushed until the scheduled time. However, if there is an urgent update required, select the **Update Now** button.
Update Now	Select to manually initiate an FDN update.
Submit attack characteristics... (recommended)	Select to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.

Manual updates

To manually update the signature definitions file, you need to first go to the Support web site at https://support.fortinet.com. Once logged in, select FortiGuard Service Updates from the Download area of the web page. The browser will present you the most current antivirus and IPS signature definitions which you can download.

Once downloaded to your computer, log into the FortiGate unit to load the definition file.

To load the definition file onto the FortiGate unit

1. Go to **System > Config > FortiGuard**.
2. Select the **Update** link for either **AV Definitions or IPS Definitions**.

3. Locate the downloaded file and select **OK**.

The upload may take a few minutes to complete.

Automatic updates

The FortiGate unit can be configured to request updates from the FortiGuard Distribution Network. You can configure this to be on a scheduled basis, or with push notifications.

Scheduling updates

Scheduling updates ensures that the virus and IPS definitions are downloaded to your FortiGate unit on a regular basis, ensuring that you do not forget to check for the definition files yourself. As well, by scheduling updates during off-peak hours, such as evenings or weekends, when network usage is minimal, ensures that the network activity will not suffer from the added traffic of downloading the definition files.

If you require the most up-to-date definitions as viruses and intrusions are found in the wild, the FortiGuard Distribution Network can push updates to the FortiGate units as they are developed. This ensures that your network will be protected from any breakouts of a virus within the shortest amount of time, minimizing any damaging effect that can occur. Push updates require that you have registered your FortiGate unit.

Once push updates are enabled, the next time new antivirus or IPS attack definitions are released, the FDN notifies all the FortiGate unit that a new update is available. Within 60 seconds of receiving a push notification, the unit automatically requests the update from the FortiGuard servers.

To enable scheduled updates - web-based manager

1. Go to **System > Config > FortiGuard**.
2. Click the Expand Arrow for **AV and IPS Options**.
3. Select the **Scheduled Update** check box.
4. Select the frequency of the updates and when within that frequency.
5. Select **Apply**.

To enable scheduled updates - CLI

```
config system autoupdate schedule
   set status enable
   set frequency {every | daily | weekly}
   set time <hh:mm>
   set day <day_of_week>
end
```

Push updates

Push updates enable you to get immediate updates when new virus or intrusions have been discovered and new signatures are created. This ensures that when the latest signature is available it will be sent to the FortiGate.

When a push notification occurs, the FortiGuard server sends a notice to the FortiGate unit that there is a new signature definition file available. The FortiGate unit then initiates a download of the definition file, similar to the scheduled update.

To ensure maximum security for your network, you should have a scheduled update as well as enable the push update, in case an urgent signature is created, and your cycle of the updates only occurs weekly.

To enable push updates - web-based manager

1. Go to **System > Config > FortiGuard**.
2. Click the Expand Arrow for **AV and IPS Options**.
3. Select **Allow Push Update**.
4. Select **Apply**.

To enable push updates - CLI

```
config system autoupdate push-update
   set status enable
end
```

Push IP override

If the FortiGate unit is behind another NAT device (or another FortiGate unit), to ensure it receives the push update notifications, you need to use an override IP address for the notifications. To do this, you create a virtual IP to map to the external port of the NAT device.

Generally speaking, if there are two FortiGate devices as in the diagram below, the following steps need to be completed on the FortiGate NAT device to ensure the FortiGate unit on the internal network receives the updates:

- Add a port forwarding virtual IP to the FortiGate NAT device that connects to the Internet by going to **Firewall Objects > Virtual IP**.
- Add a security policy to the FortiGate NAT device that connects to the Internet that includes the port forwarding virtual IP.
- Configure the FortiGate unit on the internal network with an override push IP and port.

On the FortiGate internal device, the virtual IP is entered as the **Use push override IP** address.

To enable push update override- web-based manager

1. Go to **System > Config > FortiGuard**.
2. Click the Expand Arrow for **AV and IPS Options**.
3. Select **Allow Push Update**.
4. Select **Use push override IP**.
5. Enter the virtual IP address configured on the NAT device.
6. Select **Apply**.

To enable push updates - CLI

```
config system autoupdate push-update
   set status enable
   set override enable
   set address <vip_address>
end
```

Configuring Web Filtering and Email Filtering Options

Go to **System > Config > FortiGuard**, and expand arrow to view **Web Filtering and Email Filtering Options** for setting the size of the caches and ports used.

Web Filter cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Antispam cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Port Section	Select the port assignments for contacting the FortiGuard servers. Select the **Test Availability** button to verify the connection using the selected port.
To have a URL's category rating re-evaluated, please click here	Select to re-evaluate a URL's category rating on the FortiGuard Web Filter service.

Email filtering

The FortiGuard data centers monitor and update email databases of known spam sources. With FortiGuard Antispam enabled, the FortiGate unit verifies incoming email sender address and IPs against the database, and take the necessary action as defined within the antivirus profiles.

Spam source IP addresses can also be cached locally on the FortiGate unit, providing a quicker response time, while easing load on the FortiGuard servers, aiding in a quicker response time for less common email address requests.

By default, the antispam cache is enabled. The cache includes a time-to-live value, which is the amount of time an email address will stay in the cache before expiring. You can change this value to shorten or extend the time between 300 and 86400 seconds.

To modify the antispam filter cache size - web-based manager

1. Go to **System > Config > FortiGuard**.
2. Click the Expand Arrow for **Web Filtering and Email Filtering Options**.
3. Enter the TTL value for the **antispam cache**.
4. Select **Apply**.

To modify the web filter cache size - CLI

```
config system fortiguard
   set antispam-cache-ttl <integer>
end
```

Further antispam filtering options can be configured to block, allow or quarantine, specific email addresses. These configurations are available through the **Security Profiles > Antispam** menu. For more information, see the Security Profiles handbookchapter.

Online Security Tools

The FortiGuard online center provides a number of online security tools that enable you to verify or check ratings of web sites, email addresses as well as check file for viruses:

- **URL lookup** - By entering a web site address, you can see if it has been rated and what category and classification it is filed as. If you find your web site or a site you commonly go to has been wrongly categorized, you can use this page to request that the site be re-evaluated.
  http://www.fortiguard.com/webfiltering/webfiltering.html
- **IP and signature lookup** - The IP and signature lookup enables you to check whether an IP address is blacklisted in the FortiGuard IP reputation database or whether a URL or email address is in the signature database.
  http://www.fortiguard.com/antispam/antispam.html
- **Online virus scanner** - If you discover a suspicious file on your machine, or suspect that a program you downloaded from the Internet might be malicious you can scan it using the FortiGuard online scanner. The questionable file can be uploaded from your computer to a dedicated server where it will be scanned using FortiClient Antivirus. Only one file of up to 1 MB can be checked at any one time. All files will be forwarded to our research labs for analysis.
  http://www.fortiguard.com/antivirus/virus_scanner.html
- **Malware removal tools** - Tools have been developed by FortiGuard Labs to disable and remove the specific malware and related variants. Some tools have been developed to remove specific malware, often tough to remove. A universal cleaning tool, FortiCleanup, is also available for download.
  The FortiCleanup is a tool developed to identify and cleanse systems of malicious rootkit files and their associated malware. Rootkits consist of code installed on a system with kernel level privileges, often used to hide malicious files, keylog and thwart detection / security techniques. The aim of this tool is to reduce the effectiveness of such malware by finding and eliminating rootkits. The tool offers a quick memory scan as well as a full system scan. FortiCleanup will not only remove malicious files, but also can cleanse registry entries, kernel module patches, and other tricks commonly used by rootkits - such as SSDT hooks and process enumeration hiding.
  A license to use these applications is provided free of charge, courtesy of Fortinet.
  http://www.fortiguard.com/antivirus/malware_removal.html

FortiCloud

FortiCloud (formerly known as FAMS) is a hosted security management and log retention service for FortiGate devices. It gives you centralized reporting, traffic analysis, configuration management and log retention without the need for additional hardware and software.

FortiGate models 800 and above do not support the FortiCloud service.

FortiCloud offers a wide range of features:

- **Simplified central management** - FortiCloud provides a central web-based management console to manage individual or aggregated FortiGate and FortiWiFi devices. Adding a device to the FortiCloud management subscription is straightforward and provides detailed traffic and application visibility across the whole network.

- **Hosted log retention with large default storage allocated** - Log retention is an integral part of any security and compliance program but administering a separate storage system is burdensome. FortiCloud takes care of this automatically and stores the valuable log information in the cloud. Each device is allowed up to 200Gb of log retention storage. Different types of logs can be stored including Traffic, System Events, Web, Applications and Security Events.
- **Monitoring and alerting in real time** - Network availability is critical to a good end-user experience. FortiCloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.
- **Customized or pre-configured reporting and analysis tools** - Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. For example, you may want to look closely at application usage or web site violations. The reports can be emailed as PDFs and can cover different time periods.
- **Maintain important configuration information uniformly** - The correct configuration of the devices within your network is essential to maintaining an optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.
- **Service security** - All communication (including log information) between the devices and the clouds is encrypted. Redundant data centers are always used to give the service high availability. Operational security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

Registration and Activation

Before you can activate a FortiCloud account, you must first register your device.

FortiCloud accounts can be registered manually through the FortiCloud website, https://www.forticloud.com, but you can easily register and activate your account directly within your FortiGate unit. Your registration process will vary somewhat, depending on which firmware version and device you have.

FortiGate models 300 and below, all FortiWiFi units

1. On your device's dashboard, in the License Information widget, select the green **Activate** button in the FortiCloud section.
2. A dialogue asking you to register your FortiCloud account will appear. Enter your information, view and accept the Terms and Conditions and select **Create Account**.
3. A second dialogue window will appear, asking you to enter your information to confirm your account. This will send a confirmation email to your registered email. The dashboard widget will update to show that confirmation is required.
4. Open your email, and follow the confirmation link contained in it.

A FortiCloud page will open, stating that your account has been confirmed. The Activation Pending message on the dashboard will change to state the type of account you have ('1Gb Free' or '200Gb Subscription'), and will now provide a link to the FortiCloud portal.

FortiGate models 600 to 800

For 600 through 800, FortiCloud registration must be done through the FortiGate CLI Console.

Enabling logging to FortiCloud

1. Go to **Log & Report > Log Config > Log Settings**.
2. Enable **Send Logs to FortiCloud.**
3. Select **Test Connectivity** to ensure that your FortiGate can connect to the registered FortiCloud account.

Logging into the FortiCloud portal

Once logging has been configured and you have registered your account, you can log into the FortiCloud portal and begin viewing your logging results. There are two methods to reach the FortiCloud portal:

- If you have direct networked access to the FortiGate unit, you can simply open your Dashboard and check the License Information widget. Next to the current FortiCloud connection status will be a link to reach the FortiCloud Portal.
- If you do not currently have access to the FortiGate's interface, you can visit the FortiCloud website (https://forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiCloud account you are connecting to and then you will be granted access. Connected devices can be remotely configured using the Scripts page in the Management Tab, useful if an administrator may be away from the unit for a long period of time.

Upgrading to a 200Gb subscription

Upgrading your subscription is simple but must be done through the FortiGate unit, as the storage contract is allocated based on devices rather than user accounts.

1. Open the FortiGate Dashboard.
2. In the License Information widget, select **Upgrade** next to 'Type' in the FortiCloud section.
3. A new window will open, showing the Fortinet Support portal. Follow the on-screen instructions to register your contract.
4. Wait approximately 10 minutes for the contract to be applied and then visit your Dashboard.

In the License Information widget, Type will have changed from 'Free' to 'Subscribed'. Your maximum listed storage will also have updated.

Cloud Sandboxing

FortiCloud can be used for automated sample tracking, or sandboxing, for files from a FortiGate unit. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. This feature was formerly known as FortiGuard Analytics.

Cloud sandboxing is configured by going to **System > Config > FortiSandbox**. After enabling FortiSandbox, select **Cloud Sandbox (FortiCloud).**

Sandboxing results will be shown in a new tab called **AV Submissions** in the FortiCloud portal. This tab will only appear after a file has been sent for sandboxing.

Administrators

By default, the FortiGate unit has a super administrator called "admin". This user login cannot be deleted and always has ultimate access over the FortiGate unit. Additional administrators can be added for various functions, each with a unique username, password, and set of access privileges.

There are two levels of administrator accounts; regular administrators and system administrators. Regular administrators are administrators with any admin profile other than the default super_admin. System administrators are administrators that are assigned the super_admin profile, which has the highest level of access.

Adding administrators

The name of the administrator should not contain the characters <> () #" '. Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.

Only the default ”admin” account or an administrator with read-write access control to add new administrator accounts and control their permission levels can create a new administrator account. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

When adding administrators, you are setting up the administrator’s user account. An administrator account comprises of an administrator’s basic settings as well as their access profile. The access profile is a definition of what the administrator is capable of viewing and editing.

To add an administrator - web-based manager

1. Go to **System > Admin > Administrators**.
2. Select **Create New**.
3. Enter the administrator name.
4. Select the type of account it will be. If you select **Remote**, the FortiGate unit can reference a RADIUS, LDAP or TACAS+ server.
5. When selecting **Remote** or **PKI** accounts, select the User Group the account will access.
   For information on logging in using remote authentication servers, see the User Authentication Guide. For an example of setting up a user with LDAP, see LDAP Admin Access and Authorization on page 223
6. Enter the password for the user.
   This may be a temporary password that the administrator can change later. Passwords can be up to 256 characters in length. For more information on passwords, see Passwords on page 232.
7. Select **OK**.

To add an administrator - CLI

```
config system admin
   edit <admin_name>
      set password <password>
      set accprofile <profile_name>
end
```

LDAP Admin Access and Authorization

You can use the LDAP server as a means to add administrative users, saving the time to add users to the FortiGate unit administrator list. After configuring, any user within the selected LDAP group server can automatically log into the FortiGate unit as an adm i st rat or. Ensure that the admin profile is the correct level of access, or the users within the LDAP group are the only ones authorized to configure or modify the configuration of the FortiGate unit.

To do this, requires three steps:

- configure the LDAP server
- add the LDAP server to a user group
- configure the administrator account

Configure the LDAP server

First set up the LDAP server as you normally would, and include a group to bind to.

To configure the LDAP server - web-based manager

1. Go to **User & Device > Remote > LDAP** and select **Create New**.
2. Enter a **Name** for the server.
3. Enter the **Server IP** address or name.
4. Enter the **Common Name Identifier** and **Distinguished Name**.
5. Set the **Bind Type to Regular** and enter the **User DN** and **Password**.
6. Select **OK**.

To configure the LDAP server - CLI

```
config user ldap
   edit <ldap_server_name>
      set server <server_ip>
      set cnid cn
      set dn DC=XYZ,DC=COM
      set type regular
      set username CN=Administrator,CN=Users,DC=XYZ,DC=COM
      set password <password>
      set member-attr <group_binding>
end
```

Add the LDAP server to a user group

Next, create a user group that will include the LDAP server that was created above.

To create a user group - web-based manager

1. Go to **User & Device > User Group > User Group** and select **Create New**.
2. Enter a **Name** for the group.
3. In the section labelled **Remote authentication servers**, select **Add**.
4. Select the **Remote Server** from the drop-down list.
5. Select **OK**.

To create a user group - CLI

```
config user group
   edit <group_name>
      config match
         edit 1
            set server-name <LDAP_server>
            set group-name <group_name>
```

```
      end
   end
```

Configure the administrator account

Now you can create a new administrator, where rather than entering a password, you will use the new user group and the wildcard option for authentication.

To create an administrator - web-based manager

1. Go to **System > Admin > Administrators** and select **Create New**.
2. In the **Administrator** field, enter the name for the administrator.
3. For **Type**, select **Remote**.
4. Select the **User Group** created above from the drop-down list.
5. Select **Wildcard**.
6. The Wildcard option allows for LDAP users to connect as this administrator.
7. Select an **Admin Profile**.
8. Select **OK**.

To create an administrator - CLI

```
config system admin
   edit <admin_name>
      set remote-auth enable
      set accprofile super_admin
      set wildcard enable
      set remote-group ldap
   end
```

Monitoring administrators

You can view the administrators logged in using the **System Information** widget on the Dashboard. On the widget is the **Current Administrator** row that shows the administrator logged in and the total logged in. Selecting **Details** displays the administrators), where they are logging in from and how (CLI, web-based manager) and when they logged in.

You are also able to monitor the activities the administrators perform on the FortiGate unit using the logging of events. Event logs include a number of options to track configuration changes.

To set logging - web-based manager

1. Go to **Log & Report > Log Config > Log Settings**.
2. Under **Event Logging**, ensure **System activity event** is selected.
3. Select **Apply**.

To set logging - CLI

```
config log eventfilter
   set event enable
   set system enable
end
```

To view the logs go to **Log & Report > Event Log**.

Administrator profiles

Administer profiles define what the administrator user can do when logged into the FortiGate unit. When you set up an administrator user account, you also assign an administrator profile, which dictates what the administrator user will see. Depending on the nature of the administrator's work, access level or seniority, you can allow them to view and configure as much, or as little, as required.

super_admin profile

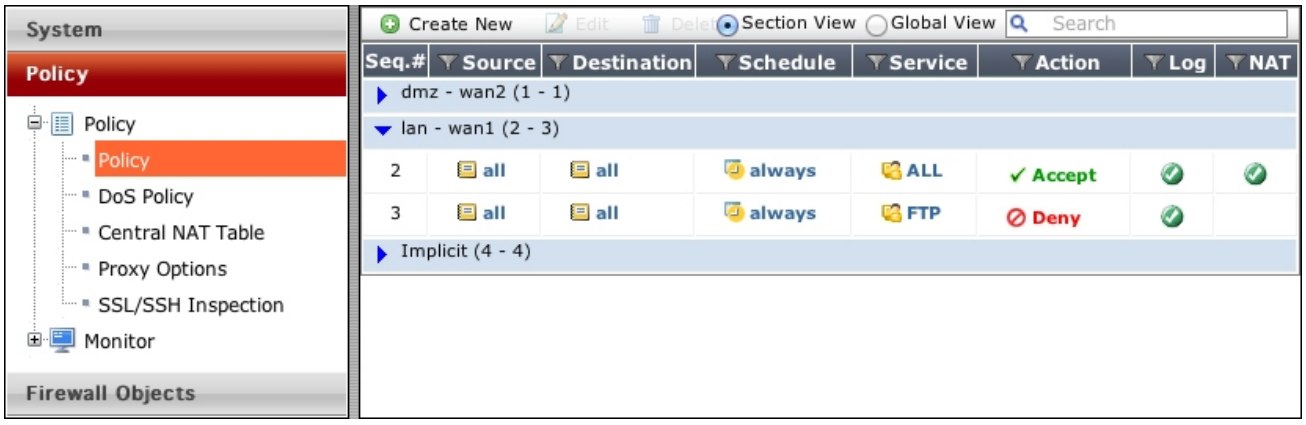
The super_admin administrator is the administrative account that the primary administrator should have to log into the FortiGate unit. The profile can not be deleted or modified to ensure there is always a method to administer the FortiGate unit.This user profile has access to all components of FortiOS, including the ability to add and remove other system administrators. For some administrative functions, such as backing up and restoring the configuration using SCP, super_admin access is required.

Creating profiles

To configure administrator profiles go to **System > Admin > Admin Profiles**. You can only assign one profile to an administrator user.

On the **New Admin Profile** page, you define the components of FortiOS that will be available to view and/or edit. For example, if you configure a profile so that the administrator can only access the firewall components, when an administrator with that profile logs into the FortiGate unit, they will only be able to view and edit any firewall components including policies, addresses, schedules and any other settings that directly affect security policies.

The view of an administrator with firewall-only access



Global and vdom profiles

By default, when you add a new administrative profile, it is set to have a vdom scope. That is, only the super_admin has a global profile that enables configuration of the entire FortiGate unit.

There may be instances where additional global administrative profiles may be required. To add more global profiles, use the following CLI command to set or change an administrative profile to be global.

```
config system accprofile
```

```
    set scope global
      ...
end
```

Once the scope is set, you can enable the read and read/write settings.

Regular (password) authentication for administrators

You can use a password stored on the local FortiGate unit to authenticate an administrator. When you select **Regular** for **Type**, you will see **Local** as the entry in the **Type** column when you view the list of administrators.

Management access

Management access defines how administrators are able to log on to the FortiGate unit to perform management tasks such as configuration and maintenance. Methods of access can include local access through the console connection or remote access over a network or modem interface using various protocols including Telnet and HTTPS.

You can configure management access on any interface in your VDOM. In NAT mode, the interface IP address is used for management access. In transparent mode, you configure a single management IP address that applies to all interfaces in your VDOM that permit management access. The FortiGate unit also uses this IP address to connect to the FDN for virus and attack updates.

The system administrator (admin) can access all VDOMs, and create regular administrator accounts. A regular administrator account can access only the VDOM to which it belongs and the management computer must connect to an interface in that VDOM. In both cases, the management computer must connect to an interface that permits management access and its IP address must be on the same network. Management access can be via HTTP, HTTPS, Telnet, or SSH sessions, if those services are enabled on the interface. HTTPS and SSH are preferred as they are more secure.

You can allow remote administration of the FortiGate unit. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid this unless it is required for your configuration. The following precautions can be taken to improve the security of a FortiGate unit that allows remote administration from the Internet:

- Use secure administrative user passwords.
- Change these passwords regularly.
- Enable two-factor authentication for administrators.
- Enable secure administrative access to this interface using only HTTPS or SSH.
- Use Trusted Hosts to limit where the remote access can originate from.
- Do not change the system idle timeout from the default value of 5 minutes.

Security Precautions

One potential point of a security breach is at the management computer. Administrators who leave their workstations for a prolonged amount of time while staying logged into the web-based manager or CLI leave the firewall open to malicious intent.

Preventing unwanted login attempts

Setting trusted hosts for an administrator limits what computers an administrator can log in from, causing the FortiGate unit to only accept the administrator's login from the configured IP address. Any attempt to log in with the same credentials from any other IP address will be dropped.

Trusted hosts are configured when adding a new administrator by going to **System > Admin > Administrators** in the web-based manager or `config system admin` in the CLI.

To ensure the administrator has access from different locations, you can enter up to ten IP addresses, though ideally this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields. Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

The trusted hosts apply to the web-based manager, ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

Prevent multiple admin sessions

Multiple admin sessions can occur when multiple users access the FortiGate using the same admin account. By default, the FortiGate unit enables multiple logins of administrators using the same login credentials from different locations. To control admin log ins, and minimize the potential of configuration collisions, you can disable concurrent admin sessions. When disabled, only one user can use the admin account at a time. When a second admin attempts to connect, connection is denied with a message that the login attempt failed.

To disable concurrent admin sessions, enter the following command in the CLI:

```
config system global
   set admin-concurrent disable
end
```

On 2U FortiGate units, this option is also available in the Web-Based Manager by going to **System > Admin > Settings** and select **Allow each admin to log in with multiple sessions**.

Segregated administrative roles

To minimize the effect of an administrator causing errors to the FortiGate configuration and possibly jeopardizing the network, create individual administrative roles where none of the administrators have super-admin permissions. For example, one admin account is used solely to create security policies, another for users and groups, another for VPN, and so on.

Disable admin services

On untrusted networks, turn off the weak administrative services such as Telnet and HTTP. With these services, passwords are passed in the clear, not encrypted. These services can be disabled by going to **System > Network > Interface** and unselecting the required check boxes.

SSH login time out

When logging into the console using SSH, the default time of inactivity is 120 seconds (2 minutes) to successfully log into the FortiGate unit. To enhance security, you can configure the time to be shorter. Using the CLI, you can change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds.

To set the logout time enter the following commands:

```
config system global
   set admin-ssh-grace-time <number_of_seconds>
end
```

Idle time-out

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out that will automatically log the user out if the web-based manager is not used for a specified amount of time. This will cause the administrator to log in to the device again in order to continue their work.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out - web-based manager

1. Go to **System > Admin > Settings**.
2. In the **Administration Settings**, enter the amount of time the Administrator login can remain idol in the **Idle Timeout** field.
3. Select **Apply**.

To set the idle time out - CLI

```
config system global
   set admintimeout <minutes>
end
```

HTTPS redirect

When selecting port numbers for various protocols, you can also enable or disable the Redirect to HTTPS option. When enabled, if you select the Administrative Access for an interface to be only HTTP, HTTPS will automatically be enabled, allowing the administrator access with either HTTP or HTTPS. The administrator can then log in using HTTPS for better security.

Note that if an SSL VPN is also configured for the same port, the SSL connection is over the HTTPS protocol. In these situations, the FortiGate unit will not redirect an HTTP address to the SSL VPN HTTPS address. Ideally, the administrator should not have the management address and an SSL VPN portal on the same interface.

Log in/out warning message

For administrators logging in and out of the FortiGate unit, you can include a login disclaimer. This disclaimer provides a statement that must be accepted or declined where corporations are governed by strict usage policies for forensics and legal reasons.

The disclaimer is enabled through the CLI.

To disable an interface:

```
config system global
   set pre-login-banner enable
   set post-login-banner enable
end
```

When set, once the administrator enters their user name and password, the disclaimer appears. They must select either Accept or Decline to proceed. When the post login is enabled, once the administrator logs out they are presented with the same message.

The banner is a default message that you can customize by going to **System > Config > Replacement Messages**. Select **Extended View** to see the **Admin** category and messages.

Disable the console interface

To prevent any unwanted login attempts using the COM communication port, you can disable login connections to the FortiGate unit.

This command is specifically for the COM port. You can still use FortiExplorer to connect and configure the FortiGate unit if required.

To disable an interface:

```
config system console
   set login disable
end
```

Disable interfaces

If any of the interfaces on the FortiGate unit are not being used, disable traffic on that interface. This avoids someone plugging in network cables and potentially causing network bypass or loop issues.

To disable an interface - web-based manager

1. Go to **System > Network > Interface**.
2. Select the interface from the list and select **Edit**.
3. For **Administrative Access**, select **Down**.
4. Select **OK**.

To disable an interface - CLI

```
config system interface
   edit <inerface_name>
      set status down
end
```

RADIUS authentication for administrators

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication and authorization functions of the RADIUS server. To use the RADIUS server for authentication, you must configure the server before configuring the FortiGate users or user groups that will need it.

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit sends the user's credentials to the RADIUS server for authentication. If the RADIUS server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the RADIUS server cannot authenticate the user, the FortiGate unit refuses the connection.

If you want to use a RADIUS server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the RADIUS server
- create the RADIUS user group

- configure an administrator to authenticate with a RADIUS server.

Configuring LDAP authentication for administrators

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, printers, etc.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. If the LDAP server cannot authenticate the administrator, the FortiGate unit refuses the connection.

If you want to use an LDAP server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure an LDAP server
- create an LDAP user group
- configure an administrator to authenticate with an LDAP server.

To view the LDAP server list, go to **User & Device > Remote > LDAP**.

For more information, see LDAP Admin Access and Authorization on page 223 .

TACACS+ authentication for administrators

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiGate unit contacts the TACACS+ server for authentication. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiGate unit.

If you want to use an TACACS+ server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication uses a certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

Passwords

Using secure admin passwords are vital for preventing unauthorized access to your FortiGate unit. When changing the password, consider the following to ensure better security:

- Do not make passwords that are obvious, such as the company name, administrator names, or other obvious word or phrase.
- Use numbers in place of letters, for example, `passw0rd`. Alternatively, spell words with extra letters, for example, **password**.
- Administrative passwords can be up to 64 characters.
- Include a mixture of letters, numbers, and upper and lower case.
- Use multiple words together, or possibly even a sentence, for example keytothehighway.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password, such as changing from `password` to `password1`.
- Write the password down and store it in a safe place away from the management computer, in case you forget it or ensure that at least two people know the password in the event that one person becomes ill, is away on vacation or leaves the company. Alternatively, have two different admin logins.

Password policy

The FortiGate unit includes the ability to enforce a password policy for administrator login. With this policy, you can enforce regular changes and specific criteria for a password including:

- minimum length between 8 and 64 characters.
- if the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- if the password must contain numbers (1, 2, 3).
- if the password must contain non-alphanumeric characters (!, @, #, $, %, ^, &, *, ().
- where the password applies (admin or IPsec or both).
- the duration of the password before a new one must be specified.

To apply a password policy - web-based manager

1. Go to **System > Admin > Settings**.
2. Select **Enable Password Policy** and configure the settings as required.

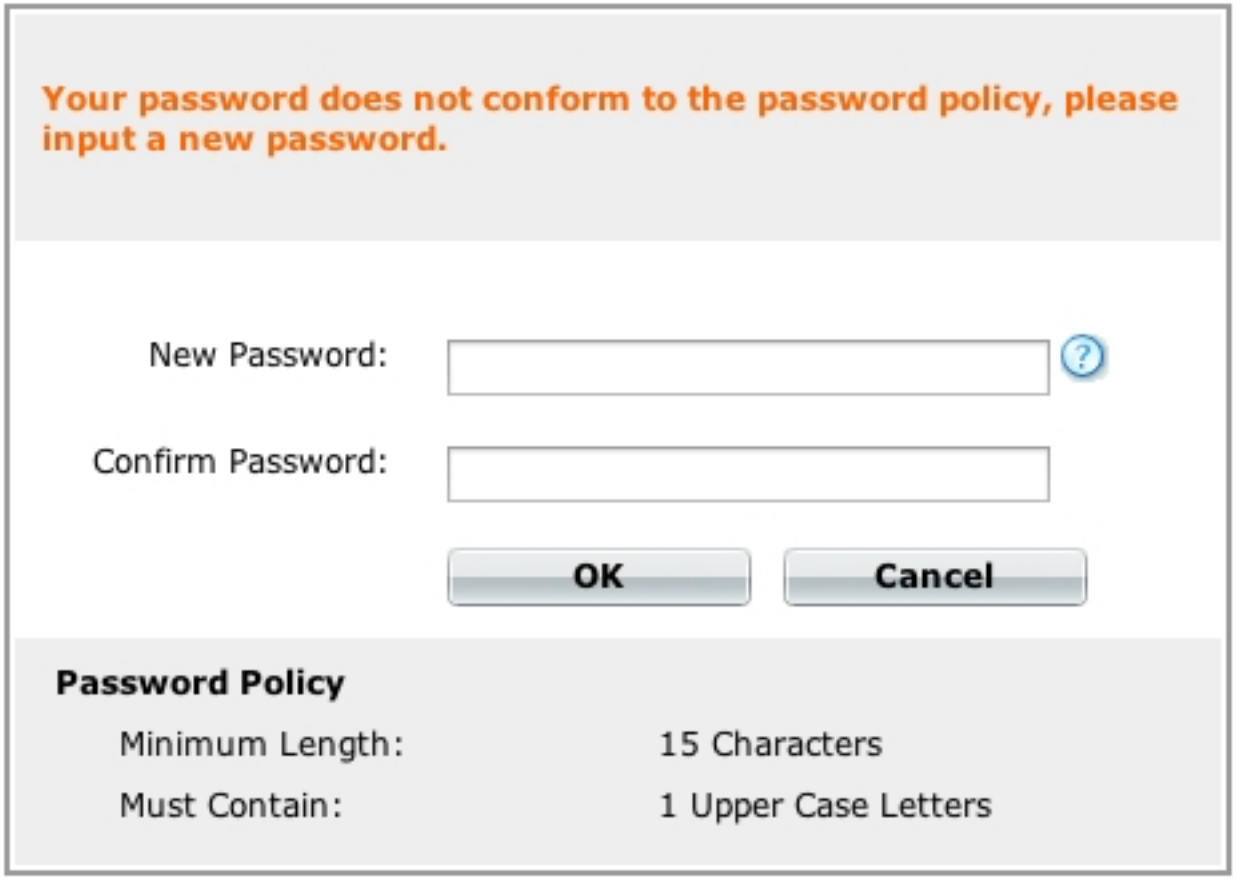
To apply a password policy - CLI

```
config system password-policy
   set status enable
```

Configure the other settings as required.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiGate unit, they are prompted to update their password to meet the new requirements before proceeding to log in.

Password policy dialog box



Lost Passwords

If an administrator password has been lost, refer to the SysAdmin's Notebook article "Resetting a lost admin password," found at docs.fortinet.com/p/sysadmin-s-notebook-and-tech-notes.

Configuration Backups

Once you configure the FortiGate unit and it is working correctly, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate unit to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it. You should also backup the local certificates, as the unique SSL inspection CA and server certificates that are generated by your FortiGate by default are not saved in a system backup.

It is also recommended that once *any* further changes are made that you backup the configuration immediately, to ensure you have the most current configuration available. Also, ensure you backup the configuration before upgrading the FortiGate unit's firmware. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site. The latter two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate unit or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

Backing up the configuration using the web-based manager

1. Go to **System > Dashboard > Status**.
2. On the **System Information** widget, select **Backup** for the **System Configuration**.
3. Select to backup to your **Local PC** or to a **USB key**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
4. If VDOMs are enabled, select to backup the entire FortiGate configuration (**Full Config**) or only a specific VDOM configuration (**VDOM Config**).
5. If backing up a VDOM configuration, select the VDOM name from the list.
6. Select **Encrypt configuration file**.
   Encryption must be enabled on the backup file to back up VPN certificates.
7. Enter a password and enter it again to confirm it. You will need this password to restore the file.
8. Select **Backup**.
9. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

Backing up the configuration using the CLI

Use the following command:

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>]
    [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
   edit <vdom_name>
```

Backup and restore the local certificates

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate unit before you enter the command.

Backing up the local certificates

Connect to the CLI and use the following command:

```
execute vpn certificate local export tftp <cert_name> <filename> <tftp_ip>
```

where:

- `<cert_name>` is the name of the server certificate.
- `<filename>` is a name for the output file.
- `<tftp_ip>` is the IP address assigned to the TFTP server host interface.

Restoring the local certificates - web-based manager

1. Move the output file from the TFTP server location to the management computer.
2. Go to **System > Certificates > Local Certificates** and select **Import**.
3. Select the appropriate **Type** of certificate and fill in any required fields.
4. Select **Browse**. Browse to the location on the management computer where the exported file has been saved, select the file and select **Open**.
5. If required, enter the **Password** needed to upload the exported file..
6. Select **OK**.

Restoring the local certificates - CLI

Connect to the CLI and use the following command:

```
execute vpn certificate local import tftp <filename> <tftp_ip>
```

Backup and restore a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. SCP is enabled using the CLI commands:

```
config system global
   set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
   set admin-scp enable
end
config vdom
   edit <vdom_name>
```

Enable SSH access on the interface

SCP uses the SSH protocol to provide secure file transfer. The interface you use for administration must allow SSH access.

To enable SSH - web-based manager:

1. Go to **System > Network > Interface**.
2. Select the interface you use for administrative access and select **Edit**.
3. In the **Administrative Access** section, select **SSH**.
4. Select **OK**.

To enable SSH - CLI:

```
config system interface
   edit <interface_name>
      set allowaccess ping https ssh
end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Using the SCP client

The FortiGate unit downloads the configuration file as `sys_conf`. Use the following syntax to download the file:

Linux

```
scp admin@<FortiGate_IP>:fgt-config <location>
```

Windows

```
pscp admin@<FortiGate_IP>:fgt-config <location>
```

The following examples show how to download the configuration file from a FortiGate-100D, at IP address 172.20.120.171, using Linux and Windows SCP clients.

Linux client example

To download the configuration file to a local directory called `~/config`, enter the following command:

```
scp admin@172.20.120.171:fgt-config ~/config
```

Enter the admin password when prompted.

Windows client example

To download the configuration file to a local directory called c:\config, enter the following command in a Command Prompt window:

```
pscp admin@172.20.120.171:fgt-config c:\config
```

Enter the admin password when prompted.

SCP public-private key authentication

SCP authenticates itself to the FortiGate unit in the same way as an administrator using SSH accesses the CLI. Instead of using a password, you can configure the SCP client and the FortiGate unit with a public-private key pair.

To configure public-private key authentication

1. Create a public-private key pair using a key generator compatible with your SCP client.
2. Save the private key to the location on your computer where your SSH keys are stored.
   This step depends on your SCP client. The Secure Shell key generator automatically stores the private key.
3. Copy the public key to the FortiGate unit using the CLI commands:

```
config system admin
   edit admin
      set ssh-public-key1 "<key-type> <key-value>"
   end
```

   `<key-type>` must be the ssh-dss for a DSA key or ssh-rsa for an RSA key. For the `<key-value>`, copy the public key data and paste it into the CLI command.

   If you are copying the key data from Windows Notepad, copy one line at a time and ensure that you paste each line of key data at the end of the previously pasted data. As well:

   - Do not copy the end-of-line characters that appear as small rectangles in Notepad.
   - Do not copy the `---- BEGIN SSH2 PUBLIC KEY ---- or Comment: "[2048-bit dsa,...]"` lines.
   - Do not copy the `---- END SSH2 PUBLIC KEY ----` line.
4. Type the closing quotation mark and press **Enter**.

Your SCP client can now authenticate to the FortiGate unit based on SSH keys rather than the administrator password.

Restoring a configuration using SCP

To restore the configuration using SCP, use the commands:

```
scp <local_file> <admin_user>@<FGT_IP>:fgt-restore-config
```

To use this command/method of restoring the FortiGate configuration, you need to log in as the “admin” administrator.

Restoring a configuration

Should you need to restore a configuration file, use the following steps:

To restore the FortiGate configuration - web-based manager

1. Go to **System > Dashboard > Status**.
2. On the **System Information** widget, select **Restore** for the **System Configuration**.

3. Select to upload the configuration file to be restored from your **Local PC or a USB key**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
4. Enter the path and file name of the configuration file, or select **Browse** to locate the file.
5. Enter a password if required.
6. Select **Restore**.

To back up the FortiGate configuration - CLI

```
execute restore config management-station normal 0
```

… or …

```
execute restore config usb <filename> [<password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_
    name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate unit will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Configuration revisions

The **Revisions** options on the **System Information** widget enables you to manage multiple versions of configuration files. Revision control requires either a configured central management server, or FortiGate units with 512 MB or more of memory. The central management server can either be a FortiManager unit or the FortiCloud.

When revision control is enabled on your unit, and configurations have been backed up, a list of saved revisions of those backed-up configurations appears.

Restore factory defaults

There may be a point where need to reset the FortiGate unit to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults. The first resets the entire device to the original out-of-the-box configuration:

To reset the FortiGate unit to its factory default settings - web-based manager

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select **Restore** for the **System Configuration**.
3. Select **Restore Factory Defaults** at the top of the page.

You can reset using the CLI by entering the command:

```
execute factoryreset
```

When prompted, type `y` to confirm the reset.

Alternatively, in the CLI you can reset the factory defaults but retain the interface and VDOM configuration.

Use the command:

```
execute factoryreset2
```

Next Steps

Now that you have installed and set up your FortiGate unit, here's a list of some resources you can read next to help you continue to get the most out of your FortiGate.

Best Practices

The Best Practices document is a collection of guidelines to ensure the most secure and reliable operation of FortiGate units in a customer environment. It is updated periodically as new issues are identified.

This document can be found at http://docs.fortinet.com/d/fortigate-best-practices.

The FortiGate Cookbook

The FortiGate Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

Using the Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

The FortiGate Cookbook can be found at http://cookbook.fortinet.com.

The Fortinet Video Library

The Fortinet Video Library contains video tutorials showing how to configure various Fortinet products, including FortiGate units. Many FortiGate videos are based on recipes from the FortiGate Cookbook.

The Fortinet Video Library can be found at http://video.fortinet.com.

The FortiOS Handbook

The FortiOS Handbook is the complete guide to FortiOS, covering a variety of FortiGate configurations.

The FortiOS Handbook is available as a single, complete document. Handbook chapters are also available as standalone documents.

The FortiOS Handbook can be found at http://docs.fortinet.com/fortigate/admin-guides.

Chapter 3 - Advanced Routing

This chapter describes advanced static routing concepts and how to implement dynamic routing on FortiGate units.

This FortiOS Handbook chapter contains the following sections:

Advanced Static Routing explains universal and static routing concepts, equal cost multipath (ECMP) and load balancing, policy routing, and routing in transparent mode.

Dynamic Routing Overview provides an overview of dynamic routing, compares static and dynamic routing, and helps you decide which dynamic routing protocol is best for you.

Routing Information Protocol (RIP) describes a distance-vector routing protocol intended for small, relatively homogeneous networks.

Border Gateway Protocol (BGP) describes classless inter-domain routing, and aggregate routes. BGP is the only routing protocol to use TCP for a transport protocol.

Open Shortest Path First (OSPF) provides background on the specific protocol explaining terms used and how the protocol works, as well as providing some troubleshooting information and examples on configuring the protocols in different situations.

Intermediate System to Intermediate System Protocol(IS-IS), which describes the link state protocol, is well-suited to smaller networks and with near universal support on routing hardware. The section also provides troubleshooting information and configuration examples.

Advanced Static Routing

Advanced static routing includes features and concepts that are used in more complex networks. Dynamic routing is not addressed in this section.

This section includes:

Routing concepts
Static routing tips
Policy routing
Transparent mode static routing
Static routing example
Advanced static routing example: ECMP failover and load balancing

Routing concepts

Many routing concepts apply to static routing. However without first understanding these basic concepts, it is difficult to understand the more complex dynamic routing.

This section includes:

- Routing in VDOMs
- Default route
- Adding a static route
- Routing table
- Building the routing table
- Static routing security
- Multipath routing and determining the best route
- Route priority
- Troubleshooting static routing

Routing in VDOMs

Routing on FortiGate units is configured per-VDOM. This means if VDOMs are enabled, you must enter a VDOM to do any routing configuration. This allows each VDOM to operate independently, with its own default routes and routing configuration.

In this guide, the procedures assume your FortiGate unit has VDOMs disabled. This is stated in the assumptions for the examples. If you have VDOMs enabled you will need to perform the following steps in addition to the procedure's steps.

To route in VDOMs - web-based manager

Select the VDOM that you want to view or configure at the bottom of the main menu.

To route in VDOMs - CLI

Before following any CLI routing procedures with VDOMs enabled, enter the following commands. For this example, it is assumed you will be working in the root VDOM. Change root to the name of your selected VDOM as needed.

```
config vdom
   edit root
```

Following these commands, you can enter any routing CLI commands as normal.

Default route

The default route is used if either there are no other routes in the routing table or if none of the other routes apply to a destination. Including the gateway in the default route gives all traffic a next-hop address to use when leaving the local network. The gateway address is normally another router on the edge of the local network.

All routers, including FortiGate units, are shipped with default routes in place. This allows customers to set up and become operational more quickly. Beginner administrators can use the default route settings until a more advanced configuration is warranted.

FortiGate units come with a default static route with an IPv4 address of 0.0.0.0, an administration distance of 10, and a gateway IPv4 address.

Adding a static route

To add or edit a static route, go to **Router > Static > Static Routes** and select **Create New**.

Destination IP / Mask	Enter the destination IP address and netmask. A value of `0.0.0.0/0.0.0.0` is universal.
Device	Select the name of the interface which the static route will connect through.
Gateway	Enter the gateway IP address.
Distance	Enter the distance value, which will affect which routes are selected first by different protocols for route management or load balancing. The default is 10.
Priority	Enter the priority if desired, which will artificially weight the route during route selection. The higher the number, the less likely the route is to be selected over others. The default is 0.

Routing table

When two computers are directly connected, there is no need for routing because each computer knows exactly where to find the other computer. They communicate directly.

Networking computers allows many computers to communicate with each other. This requires each computer to have an IP address to identify its location to the other computers. This is much like a mailing address - you will not receive your postal mail at home if you do not have an address for people to send mail to. The routing table on a computer is much like an address book used to mail letters to people in that the routing table maintains a list of

how to reach computers. Routing tables may also include information about the quality of service (QoS) of the route, and the interface associated with the route if the device has multiple interfaces.

Looking at routing as delivering letters is more simple than reality. In reality, routers loose power or have bad cabling, network equipment is moved without warning, and other such events happen that prevent static routes from reaching their destinations. When any changes such as these happen along a static route, traffic can no longer reach the destination — the route goes down. Dynamic routing can address these changes to ensure traffic still reaches its destination. The process of realizing there is a problem, backtracking and finding a route that is operational is called convergence. If there is fast convergence in a network, users won't even know that re-routing is taking place.

The routing table for any device on the network has a limited size. For this reason, routes that aren't used are replaced by new routes. This method ensures the routing table is always populated with the most current and most used routes—the routes that have the best chance of being reused. Another method used to maintain the routing table's size is if a route in the table and a new route are to the same destination, one of the routes is selected as the best route to that destination and the other route is discarded.

Routing tables are also used in unicast reverse path forwarding (uRPF). In uRPF, the router not only looks up the destination information, but also the source information to ensure that it exists. If there is no source to be found, then that packet is dropped because the router assumes it to be an error or an attack on the network.

The routing table is used to store routes that are learned. The routing table for any device on the network has a limited size. For this reason, routes that aren't used are replaced by new routes. This method ensures the routing table is always populated with the most current and most used routes — the routes that have the best chance of being reused. Another method used to maintain the routing table's size is if a route in the table and a new route are to the same destination, one of the routes is selected as the best route to that destination and the other route is discarded.

Some actions you can perform on the routing table include:

- Viewing the routing table in the web-based manager
- Viewing the routing table in the CLI
- Searching the routing table

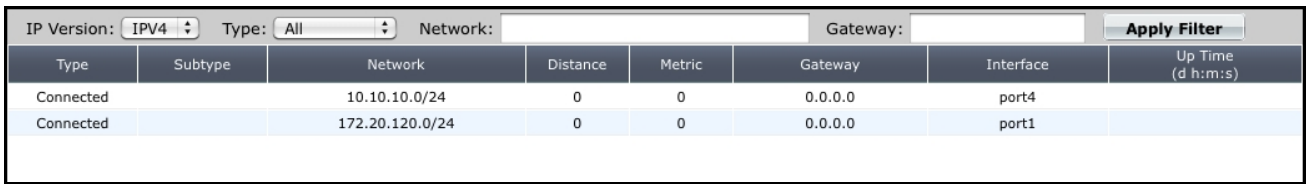
Viewing the routing table in the web-based manager

By default, all routes are displayed in the Routing Monitor list. The default static route is defined as 0.0.0.0/0, which matches the destination IP address of "any/all" packets.

To display the routes in the routing table, go to **Router > Monitor > Routing Monitor**.

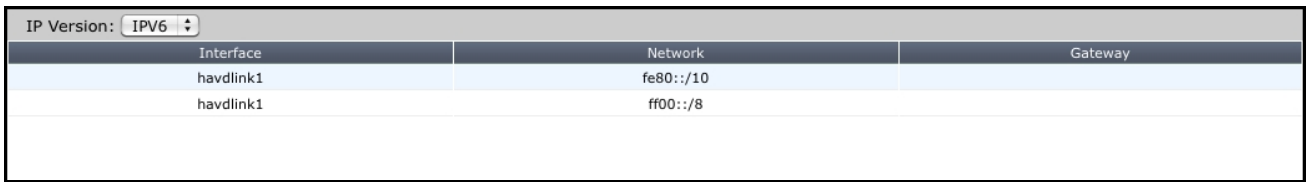
The figure below shows the Routing Monitor list belonging to a FortiGate unit that has interfaces named "port1", "port4", and "lan". The names of the interfaces on your FortiGate unit may be different.

Routing Monitor list - IPv4



The following figure shows the Routing Monitor list when IPv6 has been selected. Note that the information available for IPv6 is limited.

Routing Monitor list - IPv6



IP Version	Select IPv4 or IPv6. This is available only when IPv6 is enabled in the web-based manager. The fields displayed in the table depend on which IP version is selected.
Type	The type values assigned to FortiGate unit routes (Static, Connected, RIP, OSPF, or BGP). **All** — all routes recorded in the routing table. **Connected** — all routes associated with direct connections to FortiGate unit interfaces. **Static** — the static routes that have been added to the routing table manually. **RIP** — all routes learned through RIP. For more information see Routing Information Protocol (RIP) on page 295. **RIPNG** — all routes learned through RIP version 6 (which enables the sharing of routes through IPv6 networks). **BGP** — all routes learned through BGP. For more information see Border Gateway Protocol (BGP) on page 332. **OSPF** — all routes learned through OSPF. For more information see Open Shortest Path First (OSPF) on page 371. **OSPF6** — all routes learned through OSPF version 6 (which enables the sharing of routes through IPv6 networks). **IS-IS** — all routes learned through IS-IS. For more information see Intermediate System to Intermediate System Protocol(IS-IS) on page 412. **HA** — RIP, OSPF, and BGP routes synchronized between the primary unit and the subordinate units of a high availability (HA) cluster. HA routes are maintained on subordinate units and are visible only if you are viewing the router monitor from a virtual domain that is configured as a subordinate virtual domain in a virtual cluster. Not displayed when IP version IPv6 is selected. For details about HA routing synchronization, see the FortiGate HA User Guide.

Subtype	If applicable, the subtype classification assigned to OSPF routes. An empty string implies an intra-area route. The destination is in an area to which the FortiGate unit is connected. **OSPF inter area** — the destination is in the OSPF AS, but the FortiGate unit is not connected to that area. **External 1** — the destination is outside the OSPF AS. This is known as OSPF E1 type. The metric of a redistributed route is calculated by adding the external cost and the OSPF cost together. **External 2** — the destination is outside the OSPF AS. This is known as OSPF E2 type. In this case, the metric of the redistributed route is equivalent to the external cost only, expressed as an OSPF cost. **OSPF NSSA 1** — same as External 1, but the route was received through a not-so-stubby area (NSSA). **OSPF NSSA 2** — same as External 2, but the route was received through a not-so-stubby area. For more information on OSPF subtypes, see Open Shortest Path First (OSPF) on page 371. Not displayed when IP version 6 is selected.
Network	The IP addresses and network masks of destination networks that the FortiGate unit can reach.
Gateway	The IP addresses of gateways to the destination networks.
Interface	The interface through which packets are forwarded to the gateway of the destination network.
Up Time	The total accumulated amount of time that a route learned through RIP, OSPF, or BGP has been reachable. Not displayed when IP version IPv6 is selected.
Distance	The administrative distance associated with the route. A value of 0 means the route is preferable compared to other routes to the same destination, and the FortiGate unit may routinely use the route to communicate with neighboring routers and access servers. Modifying this distance for dynamic routes is route distribution. See Border Gateway Protocol (BGP) on page 332. Not displayed when IP version 6 is selected.

Metric	The metric associated with the route type. The metric of a route influences how the FortiGate unit dynamically adds it to the routing table. The following are types of metrics and the protocols they are applied to. **Hop count** — routes learned through RIP. **Relative cost** — routes learned through OSPF. **Multi-Exit Discriminator (MED)** — routes learned through BGP. However, several attributes in addition to MED determine the best path to a destination network. For more information on BGP attributes, see Border Gateway Protocol (BGP) on page 332. By default, the MED value associated with a BGP route is zero. However, the MED value can be modified dynamically. If the value was changed from the default, the Metric column will display a non-zero value. Not displayed when IP version 6 is selected.

Viewing the routing table in the CLI

In the CLI, you can easily view the static routing table just as in the web-based manager or you can view the full routing table.

When viewing the list of static routes using the CLI command `get route static`, it is the configured static routes that are displayed. When viewing the routing table using the CLI command `get router info routing-table all`, it is the entire routing table information that is displayed including configured and learned routes of all types. The two are different information in different formats.

If VDOMs are enabled on your FortiGate unit, all routing related CLI commands must be performed within a VDOM and not in the global context.

To view the routing table

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O  - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i  - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
*  - candidate default

S*  0.0.0.0/0 [10/0] via 192.168.183.254, port2
S    1.0.0.0/8 [10/0] via 192.168.183.254, port2
S   2.0.0.0/8 [10/0] via 192.168.183.254, port2
C   10.142.0.0/23 is directly connected, port3
B   10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
C 192.168.182.0/23 is directly connected, port2
```

Examining an entry:

```
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
```

B	BGP. The routing protocol used.
10.160.0.0/23	The destination of this route including netmask.
[20/0]	20 indicates and administrative distance of 20 out of a range of 0 to 255. 0 is an additional metric associated with this route, such as in OSPF
10.142.0.74	The gateway, or next hop.
port3	The interface used by this route.
2d18h02m	How old this route is, in this case almost three days old.

To view the kernel routing table

```
# get router info kernel

tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.11.201.0/24
    pref=10.11.201.4 gwy=0.0.0.0 dev=5(external1)

tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->172.20.120.0/24
    pref=172.20.120.146 gwy=0.0.0.0 dev=6(internal)
```

The parts of the routing table entry are:

tab	Table number. This will be either 254 (unicast) or 255 (multicast).
vf	Virtual domain of the firewall. This is the vdom index number. If vdoms are not enabled, this number will be 0.
type	Type of routing connection. Valid values include: 0 - unspecific 1 - unicast 2 - local 3 - broadcast 4 - anycast 5 - multicast 6 - blackhole 7 - unreachable 8 - prohibited
proto	Type of installation. This indicates where the route came from. Valid values include: 0 - unspecific 2 - kernel 11 - ZebOS routing module 14 - FortiOS 15 - HA 16 - authentication based 17 - HA1
prio	Priority of the route. Lower priorities are preferred.
->10.11.201.0/24 **(->x.x.x.x/mask)**	The IP address and subnet mask of the destination
pref	Preferred next hop along this route
gwy	Gateway - the address of the gateway this route will use
dev	Outgoing interface index. This number is associated with the interface for this route, and if VDOMs are enabled the VDOM will be included here as well. If an interface alias is set for this interface it will also be displayed here.

Searching the routing table

You can apply a filter to search the routing table and display certain routes only. For example, you can display one or more static routes, connected routes, routes learned through RIP, OSPF, or BGP, and routes associated with the network or gateway that you specify.

If you want to search the routing table by route type and further limit the display according to network or gateway, all of the values that you specify as search criteria must match corresponding values in the same routing table

entry in order for that entry to be displayed — an implicit AND condition is applied to all of the search parameters you specify.

For example, if the FortiGate unit is connected to network 172.16.14.0/24 and you want to display all directly connected routes to network 172.16.14.0/24, you must select **Connected** from the **Type** list, type `172.16.14.0/24` in the **Network** field, and then select **Apply Filter** to display the associated routing table entry or entries. Any entry that contains the word “Connected” in its **Type** field and the specified value in the **Gateway** field will be displayed.

In this example, you will apply a filter to search for an entry for static route to 10.10.10.10/24

To search the FortiGate unit routing table in the web-based manager

1. Go to **Router > Monitor > Routing Monitor**.
2. From the **Type** list, select the type of route to display. In our example, select **Static**.
3. If you want to display routes to a specific network, type the IP address and netmask of the network in the Networks field. In our example, enter `10.10.10.10/24`.
4. If you want to display routes to a specific gateway, type the IP address of the gateway in the **Gateway** field.
5. Select **Apply Filter**.

All of the values that you specify as search criteria must match corresponding values in the same routing table entry in order for that entry to be displayed.

To search the FortiGate unit routing table in the CLI

```
FGT # get router info routing-table details 10.10.10.10
Routing entry for 10.10.10.10/24
   Known via "static", distance 10, metric 0, best
```

If there are multiple routes that match your filter, they will all be listed, with the best match at the top of the list as indicated by the word best.

Building the routing table

In the factory default configuration, the FortiGate unit routing table contains a single static default route. You can add routing information to the routing table by defining additional static routes.

It is possible that the routing table is faced with several different routes to the same destination—the IP addresses of the next-hop router specified in those routes or the FortiGate interfaces associated with those routes may vary. In this situation, the “best” route is selected from the table.

The FortiGate unit selects the “best” route for a packet by evaluating the information in the routing table. The “best” route to a destination is typically associated with the shortest distance between the FortiGate unit and the closest gateway, also known as a next-hop router. In some cases, the next best route may be selected if the best route is unavailable.

The FortiGate unit installs the best available routes in the unit’s forwarding table, which is a subset of the unit’s routing table. Packets are forwarded according to the information in the forwarding table.

Static routing security

Securing the information on your company network is a top priority for network administrators. Security is also required as the routing protocols used are internationally known standards that typically provide little or no inherent security by themselves.

The two reasons for securing your network are the sensitive and proprietary information on your network, and also your external bandwidth. Hackers not only can steal your information, but they can also steal your bandwidth. Routing is a good low level way to secure your network, even before UTM features are applied.

Routing provides security to your network in a number of ways including obscuring internal network addresses with NAT and blackhole routing, using RPF to validate traffic sources, and maintaining an access control list (ACL) to limit access to the network.

This section includes:

- Network Address Translation (NAT)
- Access Control List (ACL)
- Blackhole Route
- Reverse path lookup

Network Address Translation (NAT)

Network address translation (NAT) is a method of changing the address from which traffic appears to originate. This practice is used to hide the IP address on a company's internal networks, and helps prevent malicious attacks that use those specific addresses.

This is accomplished by the router connected to that local network changing all the IP addresses to its externally connected IP address before sending the traffic out to the other networks, such as the Internet. Incoming traffic uses the established sessions to determine which traffic goes to which internal IP address. This also has the benefit of requiring only the router to be very secure against external attacks, instead of the whole internal network as would be the case without NAT. Securing one computer is much cheaper and easier to maintain.

1. Configuring NAT on your FortiGate unit includes the following steps.
2. Configure your internal network. For example use the `10.11.101.0` subnet.
3. Connect your internal subnet to an interface on your FortiGate unit. For example use `port1`.
4. Connect your external connection, for example an ISP gateway of `172.20.120.2`, to another interface on your Fortigate unit, for example `port2`.

Configure security policies to allow traffic between port1 and port2 on your FortiGate unit, ensuring that the NAT feature is enabled.

The above steps show that traffic from your internal network will originate on the 10.11.101.0 subnet and pass on to the 172.20.120.0 network. The FortiGate unit moves the traffic to the proper subnet. In doing that, the traffic appears to originate from the FortiGate unit interface on that subnet — it does not appear to originate from where it actually came from.

NAT "hides" the internal network from the external network. This provides security through obscurity. If a hacker tries to directly access your network, they will find the Fortigate unit, but will not know about your internal network. The hacker would have to get past the security-hardened FortiGate unit to gain access to your internal network. NAT will not prevent hacking attempts that piggy back on valid connections between the internal network and the outside world. However other UTM security measures can deal with these attempts.

Another security aspect of NAT is that many programs and services have problems with NAT. Consider if someone on the Internet tries to initiate a chat with someone on the internal network. The outsider only can access the FortiGate unit's external interface unless the security policy allows the traffic through to the internal network. If allowed in, the proper internal user would respond to the chat. However if its not allowed, the request to chat will be refused or time-out. This is accomplished in the security policy by allowing or denying different protocols.

Access Control List (ACL)

An access control list (ACL) is a table of addresses that have permission to send and receive data over a router's interface or interfaces. The router maintains an ACL, and when traffic comes in on a particular interface it is buffered, while the router looks up in the ACL if that traffic is allowed over that port or not. If it is allowed on that incoming interface, then the next step is to check the ACL for the destination interface. If the traffic passes that check as well the buffered traffic is delivered to its accentuation. If either of those steps fail the ACL check, the traffic is dropped and an error message may be sent to the sender. The ACL ensures that traffic follows expected paths, and any unexpected traffic is not delivered. This stops many network attacks. However, to be effective the ACL must be kept up to date —when employees or computers are removed from the internal network their IP addresses must also be removed from the ACL. For more information on the ACL, see the router chapter of the FortiGate CLI Reference.

Blackhole Route

A blackhole route is a route that drops all traffic sent to it. It is very much like /dev/null in Linux programming.

Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network.

Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses (traffic which may be valid or malicious) can be directed to a blackhole for added security and to reduce traffic on the subnet.

The loopback interface, a virtual interface that does not forward traffic, was added to enable easier configuration of blackhole routing. Similar to a normal interface, this loopback interface has fewer parameters to configure, and all traffic sent to it stops there. Since it cannot have hardware connection or link status problems, it is always available, making it useful for other dynamic routing roles. Once configured, you can use a loopback interface in security policies, routing, and other places that refer to interfaces. You configure this feature only from the CLI. For more information, see the system chapter of the FortiGate CLI Reference.

Reverse path lookup

Whenever a packet arrives at one of the FortiGate unit's interfaces, the unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. This is also called anti-spoofing. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet as it is likely a hacking attempt.

If the destination address can be matched to a local address (and the local configuration permits delivery), the FortiGate unit delivers the packet to the local network. If the packet is destined for another network, the Fortigate unit forwards the packet to a next-hop router according to a policy route and the information stored in the FortiGate forwarding table.

Multipath routing and determining the best route

Multipath routing occurs when more than one entry to the same destination is present in the routing table. When multipath routing happens, the FortiGate unit may have several possible destinations for an incoming packet, forcing the FortiGate unit to decide which next-hop is the best one.

It should be noted that some IP addresses will be rejected by routing protocols. These are called Martian addresses. They are typically IP addresses that are invalid and not routable because they have been assigned an address by a misconfigured system, or are spoofed addresses.

Two methods to manually resolve multiple routes to the same destination are to lower the administrative distance of one route or to set the priority of both routes. For the FortiGate unit to select a primary (preferred) route, manually lower the administrative distance associated with one of the possible routes. Setting the priority on the routes is a FortiGate unit feature and may not be supported by non-Fortinet routers.

Administrative distance is based on the expected reliability of a given route. It is determined through a combination of the number of hops from the source and the protocol used. A hop is when traffic moves from one router to the next. More hops from the source means more possible points of failure. The administrative distance can be from 1 to 255, with lower numbers being preferred. A distance of 255 is seen as infinite and will not be installed in the routing table.

Here is an example to illustrate how administration distance works — if there are two possible routes traffic can take between two destinations with administration distances of 5 (always up) and 31 (sometimes not available), the traffic will use the route with an administrative distance of 5. If for some reasons the preferred route (admin distance of 5) is not available, the other route will be used as a backup.

Different routing protocols have different default administrative distances. These different administrative distances are based on a number of factors of each protocol such as reliability, speed, and so on. The default administrative distances for any of these routing protocols are configurable.

Default administrative distances for routing protocols and connections

Routing protocol	Default administrative distance
Direct physical connection	1
Static	10
EBGP	20
OSPF	110
IS-IS	115
RIP	120
IBGP	200

Another method to determine the best route is to manually change the priority of both routes in question. If the next-hop administrative distances of two routes on the FortiGate unit are equal, it may not be clear which route the packet will take. Manually configuring the priority for each of those routes will make it clear which next-hop will be used in the case of a tie. The priority for a route be set in the CLI, or when editing a specific static route, as

described in the next section. Lower priority routes are preferred. Priority is a Fortinet value that may or may not be present in other brands of routers.

All entries in the routing table are associated with an administrative distance. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the FortiGate unit compares the administrative distances of those entries first, selects the entries having the lowest distances, and installs them as routes in the FortiGate unit forwarding table. As a result, the FortiGate unit forwarding table contains only those routes having the lowest distances to every possible destination. While only static routing uses administrative distance as its routing metric, other routing protocols such as RIP can use metrics that are similar to administrative distance.

Route priority

After the FortiGate unit selects static routes for the forwarding table based on their administrative distances, the priority field of those routes determines routing preference. Priority is a Fortinet value that may or may not be present in other brands of routers.

You can configure the priority field through the CLI or the web-based manager. Priority values can range from 0 to 4 294 967 295. The route with the lowest value in the priority field is considered the best route. It is also the primary route.

To change the priority of a route - web-based manager

1. Go to **Router > Static > Static Routes**.
2. Select the route entry, and select **Edit**.
3. Select **Advanced**.
4. Enter the **Priority** value.
5. Select **OK**.

To change the priority of a route - CLI

The following command changes the priority to 5 for a route to the address `10.10.10.1` on the `port1` interface.

```
config router static
   edit 1
      set device port1
      set gateway 10.10.10.10
      set dst 10.10.10.1
      set priority 5
   end
```

If there are other routes set to priority 10, the route set to priority 5 will be preferred. If there are routes set to priorities less than 5, those other routes will be preferred instead.

In summary, because you can use the CLI to specify which sequence numbers or priority field settings to use when defining static routes, you can prioritize routes to the same destination according to their priority field settings. For a static route to be the preferred route, you must create the route using the `config router static` CLI command and specify a low priority for the route. If two routes have the same administrative distance and the same priority, then they are equal cost multipath (ECMP) routes.

Since this means there is more than one route to the same destination, it can be confusing which route or routes to install and use. However, if you have enabled load balancing with ECMP routes, then different sessions will resolve this problem by using different routes to the same address.

Troubleshooting static routing

When there are problems with your network that you believe to be static routing related, there are a few basic tools available to locate the problem.

These tools include:

- Ping
- Traceroute
- Examine routing table contents

Ping

Beyond the basic connectivity information, ping can tell you the amount of packet loss (if any), how long it takes the packet to make the round trip, and the variation in that time from packet to packet.

If there is no packet loss detected, your basic network connectivity is OK.

If there is some packet loss detected, you should investigate:

- Possible ECMP, split horizon, network loops
- Cabling to ensure no loose connections

If there is total packet loss, you should investigate:

- Hardware - ensure cabling is correct, and all equipment between the two locations is accounted for
- Addresses and routes - ensure all IP addresses and routing information along the route is configured as expected
- Firewalls - ensure all firewalls are set to allow PING to pass through

To ping from a Windows PC

1. Go to a DOS prompt. Typically you go to **Start > Run**, enter `cmd` and select **OK**.
2. Enter `ping 10.11.101.100` to ping the default internal interface of the FortiGate unit with four packets.

To ping from an Apple computer

1. Open the Terminal.
2. Enter `ping 10.11.101.100`.
3. If the ping fails, it will stop after a set number of attempts. If it succeeds, it will continue to ping repeatedly. Press `Control+C` to end the attempt and see gathered data.

To ping from a Linux PC

1. Go to a command line prompt.
2. Enter "`/bin/etc/ping 10.11.101.101`".

Traceroute

Where ping will only tell you if it reached its destination and came back successfully, traceroute will show each step of its journey to its destination and how long each step takes. If ping finds an outage between two points, traceroute can be used to locate exactly where the problem is.

To use traceroute on an Windows PC

1. Go to a DOS prompt. Typically you go to **Start > Run**, enter "`cmd`" and select **OK**.
2. Enter "`tracert fortinet.com`" to trace the route from the PC to the Fortinet website.

To use traceroute from an Apple computer

1. Open the Terminal.
2. Enter `traceroute fortinet.com`.
3. The terminal will list the number of steps made. Upon reaching the destination, it will list three asterisks per line. Press `Control+C` to end the attempt.

To use traceroute on a Linux PC

1. Go to a command line prompt.
2. Enter "`/bin/etc/traceroute fortinet.com`".
   The Linux traceroute output is very similar to the MS Windows traceroute output.

Examine routing table contents

The first place to look for information is the routing table.

The routing table is where all the currently used routes are stored for both static and dynamic protocols. If a route is in the routing table, it saves the time and resources of a lookup. If a route isn't used for a while and a new route needs to be added, the oldest least used route is bumped if the routing table is full. This ensures the most recently used routes stay in the table. Note that if your FortiGate unit is in Transparent mode, you are unable to perform this step.

If the FortiGate is running in NAT mode, verify that all desired routes are in the routing table: local subnets, default routes, specific static routes, and dynamic routing protocols.

To check the routing table in the web-based manager, use the Routing Monitor — go to **Router > Monitor > Routing Monitor**. In the CLI, use the command `get router info routing-table all`.

Static routing tips

When your network goes beyond basic static routing, here are some tips to help you plan and manage your static routing.

Always configure a default route

The first thing configured on a router on your network should be the default route. And where possible the default routes should point to either one or very few gateways. This makes it easier to locate and correct problems in the network. By comparison, if one router uses a second router as its gateway which uses a fourth for its gateway and so on, one failure in that chain will appear as an outage for all the devices downstream. By using one or very few

addresses as gateways, if there is an outage on the network it will either be very localized or network-wide — either is easy to troubleshoot.

Have an updated network plan

A network plan lists different subnets, user groups, and different servers. Essentially is puts all your resources on the network, and shows how the parts of your network are connected. Keeping your plan updated will also help you troubleshoot problems more quickly when they arise.

A network plan helps your static routing by eliminating potential bottlenecks, and helping troubleshoot any routing problems that come up. Also you can use it to plan for the future and act on any changes to your needs or resources more quickly.

Plan for expansion

No network remains the same size. At some time, all networks grow. If you take future growth into account, there will be less disruption to your existing network when that growth happens. For example allocating a block of addresses for servers can easily prevent having to re-assign IP addresses to multiple servers due to a new server.

With static routing, if you group parts of your network properly you can easily use network masks to address each part of your network separately. This will reduce the amount of administration required both to maintain the routing, and to troubleshoot any problems.

Configure as much security as possible

Securing your network through static routing methods is a good low level method to defend both your important information and your network bandwidth.

- Implement NAT to obscure your IP address is an excellent first step.
- Implement black hole routing to hide which IP addresses are in use or not on your local network.
- Configure and use access control list (ACL) to help ensure you know only valid users are using the network.

All three features limit access to the people who should be using your network, and obscure your network information from the outside world and potential hackers.

Policy routing

Policy routing enables you to redirect traffic away from a static route. This can be useful if you want to route certain types of network traffic differently. You can use incoming traffic's protocol, source address or interface, destination address, or port number to determine where to send the traffic. For example, generally network traffic would go to the router of a subnet, but you might want to direct SMTP or POP3 traffic directly to the mail server on that subnet.

If you have configured the FortiGate unit with routing policies and a packet arrives at the FortiGate unit, the FortiGate unit starts at the top of the Policy Route list and attempts to match the packet with a policy. If a match is found and the policy contains enough information to route the packet (a minimum of the IP address of the next-hop router and the FortiGate interface for forwarding packets to it), the FortiGate unit routes the packet using the information in the policy. If no policy route matches the packet, the FortiGate unit routes the packet using the routing table.

Most policy settings are optional,and a matching policy alone might not provide enough information for forwarding the packet. In fact, the FortiGate almost always requires a matching route in the routing table in order to use a policy route. The FortiGate unit will refer to the routing table in an attempt to match the information in the packet header with a route in the routing table.

Policy route options define which attributes of a incoming packet cause policy routing to occur. If the attributes of a packet match all the specified conditions, the FortiGate unit routes the packet through the specified interface to the specified gateway.

To view policy routes go to **Router > Static > Policy Routes**.

Create New	Add a policy route. See Adding a policy route on page 259.
Edit	Edit the selected policy route.
Delete	Delete the selected policy route.
Move To	Move the selected policy route. Enter the new position and select **OK**. For more information, see Moving a policy route on page 262.
#	The ID numbers of configured route policies. These numbers are sequential unless policies have been moved within the table.
Incoming	The interfaces on which packets subjected to route policies are received.
Outgoing	The interfaces through which policy routed packets are routed.
Source	The IP source addresses and network masks that cause policy routing to occur.
Destination	The IP destination addresses and network masks that cause policy routing to occur.

Adding a policy route

To add a policy route, go to **Router > Static > Policy Route** and select **Create New**.

Protocol	Enter the protocol number to match. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers here. The range is from 0 to 255. A value of `0` disables the feature. Commonly used **Protocol** settings include 6 for TCP sessions, 17 for UDP sessions, 1 for ICMP sessions, 47 for GRE sessions, and 92 for multicast sessions.
Incoming Interface	Select the name of the interface through which incoming packets subjected to the policy are received.
Source Address / Mask	To perform policy routing based on IP source address, type the source address and network mask to match. A value of `0.0.0.0/0.0.0.0` disables the feature.
Destination Address / Mask	To perform policy routing based on the IP destination address of the packet, type the destination address and network mask to match. A value of `0.0.0.0/0.0.0.0` disables the feature.
Destination Ports	To perform policy routing based on the port on which the packet is received, type the same port number in the From and To fields. To apply policy routing to a range of ports, type the starting port number in the From field and the ending port number in the To field. A value of 0 disables this feature. The Destination Ports fields are only used for TCP and UDP protocols. The ports are skipped over for all other protocols.
Type of Service	Use a two digit hexadecimal bit pattern to match the service, or use a two digit hexadecimal bit mask to mask out. For more information, see Type of Service on page 261.
Outgoing Interface	Select the name of the interface through which packets affected by the policy will be routed.
Gateway Address	Type the IP address of the next-hop router that the FortiGate unit can access through the specified interface.

Example policy route

Configure the following policy route to send all FTP traffic received at `port1` out the `port10` interface and to a next hop router at IP address `172.20.120.23`. To route FTP traffic set protocol to 6 (for TCP) and set both of the destination ports to 21, the FTP port.

Protocol	6
Incoming interface	port1
Source address / mask	0.0.0.0/0.0.0.0
Destination address / mask	0.0.0.0/0.0.0.0
Destination Ports	From 21 to 21
Type of Service	bit pattern: 00 (hex) bit mask: 00 (hex)
Outgoing interface	port10
Gateway Address	172.20.120.23

Type of Service

Type of service (TOS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, with such qualities as delay, priority, reliability, and minimum cost.

Each quality helps gateways determine the best way to route datagrams. A router maintains a ToS value for each route in its routing table. The lowest priority TOS is 0, the highest is 7 - when bits 3, 4, and 5 are all set to 1. The router tries to match the TOS of the datagram to the TOS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero TOS route.

Using increased quality may increase the cost of delivery because better performance may consume limited network resources. For more information, see RFC 791 and RFC 1349.

The role of each bit in the IP header TOS 8-bit field

bits 0, 1, 2	**Precedence**	Some networks treat high precedence traffic as more important traffic. Precedence should only be used within a network, and can be used differently in each network. Typically you do not care about these bits.
bit 3	**Delay**	When set to 1, this bit indicates low delay is a priority. This is useful for such services as VoIP where delays degrade the quality of the sound.
bit 4	**Throughput**	When set to 1, this bit indicates high throughput is a priority. This is useful for services that require lots of bandwidth such as video conferencing.
bit 5	**Reliability**	When set to 1, this bit indicates high reliability is a priority. This is useful when a service must always be available such as with DNS servers.
bit 6	**Cost**	When set to 1, this bit indicates low cost is a priority. Generally there is a higher delivery cost associated with enabling bits 3,4, or 5, and bit 6 indicates to use the lowest cost route.
bit 7	**Reserved for future use**	Not used at this time.

For example, if you want to assign low delay, and high reliability, say for a VoIP application where delays are unacceptable, you would use a bit pattern of xxx1x1xx where an 'x' indicates that bit can be any value. Since all bits are not set, this is a good use for the bit mask; if the mask is set to 0x14, it will match any TOS packets that are set to low delay and high reliability.

Moving a policy route

A routing policy is added to the bottom of the routing table when it is created. If you prefer to use one policy over another, you may want to move it to a different location in the routing policy table.

The option to use one of two routes happens when both routes are a match, for example `172.20.0.0/255.255.0.0` and `172.20.120.0/255.255.255.0`. If both of these routes are in the policy table, both can match a route to `172.20.120.112` but you consider the second one as a better match. In that case the best match route should be positioned before the other route in the policy table.

To change the position of a policy route in the table, go to **Router > Static > Policy Routes** and select **Move To** for the policy route you want to move.

Before/After	Select Before to place the selected Policy Route before the indicated route. Select After to place it following the indicated route.
Policy route ID	Enter the Policy route ID of the route in the Policy route table to move the selected route before or after.

Transparent mode static routing

FortiOS operating modes allow you to change the configuration of your FortiGate unit depending on the role it needs to fill in your network.

NAT/Route operating mode is the standard mode where all interfaces are accessed individually, and traffic can be routed between ports to travel from one network to another.

In transparent operating mode, all physical interfaces act like one interface. The FortiGate unit essentially becomes a bridge — traffic coming in over any interface is broadcast back out over all the interfaces on the FortiGate unit.

In transparent mode, there is no entry for routing at the main level of the menu on the web-based manager display as there is in NAT/Route mode. Routing is instead accessed through the network menu option.

To view the routing table in transparent mode, go to **System > Network > Routing Table**.

When viewing or creating a static route entry in transparent mode there are only three fields available.

Destination IP / Mask	The destination of the traffic being routed. The first entry is attempted first for a match, then the next, and so on until a match is found or the last entry is reached. If no match is found, the traffic will not be routed. Use 0.0.0.0 to match all traffic destinations. This is the default route.
Gateway	Specifies the next hop for the traffic. Generally the gateway is the address of a router on the edge of your network.
Priority	The priority is used if there is more than one match for a route. This allows multiple routes to be used, with one preferred. If the preferred route is unavailable the other routes can be used instead. Valid range of priority can be from 0 to 4 294 967 295. If more than one route matches and they have the same priority it becomes an ECMP situation and traffic is shared among those routes. See Transparent mode static routing on page 262.

When configuring routing on a FortiGate unit in transparent mode, remember that all interfaces must be connected to the same subnet. That means all traffic will be coming from and leaving on the same subnet. This is important because it limits your static routing options to only the gateways attached to this subnet. For example, if you only have one router connecting your network to the Internet then all static routing on the FortiGate unit will use that gateway. For this reason static routing on FortiGate units in transparent mode may be a bit different, but it is not as complex as routing in NAT/Route mode.

Static routing example

This is an example of a typical small network configuration that uses only static routing.

This network is in a dentist office that includes a number of dentists, assistants, and office staff. The size of the office is not expected to grow significantly in the near future, and the network usage is very stable—there are no new applications being added to the network.

The users on the network are:

- Admin staff - access to local patient records, and perform online billing
- Dentists - access and update local patient records, research online from desk
- Assistants - access and update local patient records in exam rooms

The distinction here is mainly that only the admin staff and dentist's office need access to the Internet—all the other traffic is local and doesn't need to leave the local network. Routing is only required for the outbound traffic, and the computers that have valid outbound traffic.

Configuring routing only on computers that need it acts as an additional layer of security by helping prevent malicious traffic from leaving the network.

This section includes the following topics:

- Network layout and assumptions
- General configuration steps
- Configure FortiGate unit
- Configure Admin PC and Dentist PCs
- Testing network configuration

Network layout and assumptions

The computers on the network are admin staff computers, dentist office computers, and dental exam room computers. While there are other devices on the local network such as printers, they do not need Internet access or any routing.

This networked office equipment includes 1 admin staff PC, 3 dentist PCs, and 5 exam room PCs. There are also a network printer, and a router on the network as well.

Assumptions about these computers, and network include:

- The FortiGate unit is a model with interfaces labeled port1 and port2.
- The FortiGate unit has been installed and is configured in NAT/Route mode.
- VDOMs are not enabled.
- The computers on the network are running MS Windows software.
- Any hubs required in the network are not shown in the network diagram.
- The network administrator has access to the ISP IP addresses, and is the super_admin administrator on the FortiGate unit.

Static routing example device names, IP addresses, and level of access

Device Name(s)	IP address	Need external access?
Router	192.168.10.1	YES
Admin	192.168.10.11	YES
Dentist1-3	192.168.10.21-23	YES
Exam1-5	192.168.10.31-35	NO
Printer	192.168.10.41	NO

General configuration steps

The steps to configuring routing on this network are:

1. Get your ISP information such as DNS, gateway, etc.
2. Configure FortiGate unit
3. Configure Admin PC and Dentist PCs
4. Testing network configuration

Get your ISP information such as DNS, gateway, etc.

Your local network connects to the Internet through your Internet Service Provider (ISP). They have IP addresses that you need to configure your network and routing.

The addresses needed for routing are your assigned IP address, DNS servers, and the gateway.

Configure FortiGate unit

The FortiGate unit will have two interfaces in use—one connected to the internal network and one connected to the external network. Port1 will be the internal interface, and port2 will be the external interface.

To configure the FortiGate unit:

1. Configure the internal interface (port1)
2. Configure the external interface (port2)
3. Configure networking information
4. Configure basic security policies
5. Configure static routing

Configure the internal interface (port1)

To configure the internal interface (port1) - web based manager

1. Go to **System > Network > Interfaces**. Highlight **port1** and select **Edit**.
2. Enter the following:

Addressing Mode	Manual
IP/Netmask	172.100.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET
Description	Internal network

To configure the internal interface (port1) - CLI

```
config system interface
   edit port1
      set IP 192.168.10.1 255.255.255.0
      set allowaccess https ping telnet
      set description "internal network"
   end
end
```

Configure the external interface (port2)

The external interface connects to your ISP's network. You need to know the IP addresses in their network that you should connect to. Use their addresses when you get them, however for this example we will assume the address your ISP gave you is 172.100.20.20 will connect to the gateway at 172.100.20.5 on their network, and their DNS servers are 172.11.22.33 and 172.11.22.34.

To configure the internal interface (port2) - web based manager

1. Go to **System > Network > Interfaces**. Highlight **port2** and select **Edit**.
2. Enter the following:

Addressing Mode	Manual
IP/Netmask	172.100.20.20/255.255.255.0
Administrative Access	HTTPS, PING, TELNET
Description	Internal network

To configure the internal interface (port2) - CLI

```
configure system interface
   edit port2
      set IP 172.100.20.20 255.255.255.0
      set allowaccess https ping telnet
      set description "internal network"
   end
end
```

Configure networking information

Networking information includes the gateway, and DNS servers. Your FortiGate unit requires a connection to the Internet for antivirus and other periodic updates.

To configure networking information - web-based manager

1. Go to **System > Network > DNS**.
2. Enter the primary and secondary DNS addresses.
3. Select **Apply**.

To configure networking information - CLI

```
config system global
   set dns_1 172.11.22.33
   set dns_2 172.11.22.34
end
```

Configure basic security policies

For traffic to flow between the internal and external ports in both directions, two security policies are required as a minimum. More can be used to farther limit or direct traffic as needed, but will not be included here.

Before configuring the security policies, a firewall address group is configured for the PCs that are allowed Internet access. This prevents PC without Internet privileges from accessing the Internet.

The security policy assumptions are:

- Only the basic networking services have been listed as allowed for added security. Others can easily be added as the users require them.

- In this example to keep things simple, both incoming and outgoing security policies are the same. In a real network there are applications that are allowed out but not in, and vice versa.
- Endpoint control has been enabled to ensure that all computers on the local network are running FortiClient and those installs are up to date. This feature ensures added security on your local network without the need for the network administrator to continually bother users to update their software. The FortiGate unit can store an up to date copy of the FortiClient software and offer a URL to it for users to install it if they need to.

To configure security policies - web-based manager

1. Go to **Policy & Objects > Objects > Addresses**.
2. Create a new Firewall Address entry for each of:

PC Name	IP Address	Interface
Admin	192.168.10.11	port1
Dentist1	192.168.10.21	port1
Dentist2	192.168.10.22	port1
Dentist3	192.168.10.23	port1

3. Go to **Policy & Objects > Objects > Addresses**.
4. Select the dropdown arrow next to **Create New** and select **Address Group**.
5. Name the group Internet_PCs.
6. Add Admin, Dentist1, Dentist2, and Dentist3 as members of the group.
7. Select **OK**.
8. Go to **Policy & Objects > Policy > IPv4**.
9. Select **Create New**.
10. Enter the following: DH - port2(external) -> port1(internal)

Incoming Interface	port2
Source Address	all
Outgoing Interface	port1
Destination Address	Internet_PCs
Schedule	always
Service	Multiple. Select **DHCP, DNS,FTP, HTTP, HTTPS, NTP, POP3, SMTP, SSH.**
Action	ACCEPT
Log Allowed Traffic	Enabled

11. Select **OK**.
12. Select **Create New**.

13. Enter the following:

Incoming Interface	port1
Source Address	Internet_PCs
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	Multiple. Select **DHCP, DNS,FTP, HTTP, HTTPS, NTP, POP3, SMTP, SSH.**
Action	ACCEPT
Log Allowed Traffic	Enabled

14. Select **OK**.

To configure security policies - CLI

```
config firewall address
   edit "Admin"
      set associated-interface "port1"
      set subnet 192.168.10.11 255.255.255.255
   next
   edit "Dentist1"
      set associated-interface "port1"
      set subnet 192.168.10.21 255.255.255.255
   next
   edit "Dentist2"
      set associated-interface "port1"
      set subnet 192.168.10.22 255.255.255.255
   next
   edit "Dentist3"
      set associated-interface "port1"
      set subnet 192.168.10.23 255.255.255.255
   end
config firewall addrgrp
   edit Internet_PCs
      set member Admin Dentist1 Dentist2 Dentist3
   end
config firewall policy
   edit 1
      set srcintf port1
      set dstintf port2
      set srcaddr Internet_PCs
      set dstaddr all
      set action accept
      set schedule always
      set service "DHCP" "DNS" "FTP" "HTTP" "HTTPS" "NTP" "POP3" "SMTP" "SSH"
      set logtraffic enable
      set label "Section2"
```

```
        set endpoint-restrict-check no-av db-outdated
      next
      edit 2
        set srcintf port2
        set dstintf port1
        set srcaddr all
        set dstaddr Internet_PCs
        set action accept
        set schedule always
        set service "DHCP" "DNS" "FTP" "HTTP" "HTTPS" "NTP" "POP3" "SMTP" "SSH"
        set logtraffic enable
        set label "Section2"
        set endpoint-restrict-check no-av db-outdated
      end
    end
```

Configure static routing

With the rest of the FortiGate unit configured, static routing is the last step before moving on to the rest of the local network. All traffic on the local network will be routed according to this static routing entry.

To configure Fortinet unit static routing - web-based manager

1. Go to **Router > Static > Static Routes**.
2. Select **Edit** for the top route on the page.
3. Enter the following:

Destination IP/Mask	172.100.20.5
Device	port2
Gateway	172.100.20.5
Distance	10

4. Select **OK**.

To configure Fortinet unit static routing - CLI

```
config router static
  edit 1
    set gateway 172.100.20.5
    set distance 10
    set device port2
    set dst 0.0.0.0
  end
end
```

Configure Admin PC and Dentist PCs

With the router configured, next we need to configure the computers that need Internet access. These computers need routing to be configured on them. As the other computers do not require routing, they are not included here.

The procedure to configure these computers is the same. Repeat the following procedure for the corresponding PCs.

The Windows CLI procedure does not configure the DNS entries. It just adds the static routes.

To configure routing and DNS on Admin and Dentist PCs - Windows GUI

1. On PC, select **Start > Control Panel > Network Connections**.
2. Right click on the network connection to your local network that has a status of Connected, and select **Properties**.
3. Under the **General** tab, from the list select **TCP/IP**, and **Properties**.
4. Under **Gateway**, enter the FortiGate unit address (192.168.10.1).
5. Enter the primary and secondary DNS server addresses from your ISP (172.11.22.33 and 172.11.22.34).
6. Select **OK**.

To configure routing on Admin and Dentist PCs - Windows CLI

1. On PC, select **Start > Run**, enter "`cmd`", and select **OK**.
2. At the command prompt, type
   ```
   route ADD 0.0.0.0 MASK 0.0.0.0 172.100.20.5 METRIC 10
   route ADD 192.168.10.0 MASK 255.255.255.0 192.168.10.1 METRIC 5
   ```
3. Confirm these routes have been added. Type:
   ```
   route PRINT
   ```
   If you do not see the two routes you added, try adding them again paying attention to avoid spelling mistakes.
4. Test that you can communicate with other computers on the local network, and with the Internet. If there are no other computers on the local network, connect to the FortiGate unit.

Configure other PCs on the local network

The PCs on the local network without Internet access (the exam room PCs) can be configured now.

As this step does not require any routing, details have not been included.

Testing network configuration

There are three tests to run on the network to ensure proper connectivity.

- To test that PCs on the local network can communicate
- Test that Internet_PCs on the local network can access the Internet
- Test that non-Internet_PCs can not access the Internet

Test that PCs on the local network can communicate

1. Select any two PCs on the local network, such as Exam4 and Dentist3.
2. On the Exam4 PC, at the command prompt enter `ping 192.168.10.23.`
   The output from this command should appear similar to the following.

```
Pinging 192.168.10.23 with 32 bytes of data:

Reply from 192.168.10.23: bytes=32 time<1m TTL=255
Reply from 192.168.10.23: bytes=32 time<1m TTL=255
Reply from 192.168.10.23: bytes=32 time<1m TTL=255
```

3. At the command prompt enter `exit` to close the window.
4. On the Dentist3 PC, at the command prompt enter `ping 192.168.10.34.`
   The output from this command should appear similar to the following.

```
Pinging 192.168.10.34 with 32 bytes of data:

Reply from 192.168.10.34: bytes=32 time<1m TTL=255
Reply from 192.168.10.34: bytes=32 time<1m TTL=255
Reply from 192.168.10.34: bytes=32 time<1m TTL=255
```

5. At the command prompt enter `exit` to close the window.
6. Repeat these steps for all PCs on the local network.
   If the output does not appear similar to above, there is a problem with the network configuration between these two PCs.

To test that Internet_PCs on the local network can access the Internet

The easiest way to access the Internet is with an Internet browser. However, if that doesn't work its best to do a traceroute to see at what point the problem is. This can help determine if it is a networking problem such as cabling, or if its an access problem such as this PC not having Internet access.

1. Select any PC on the local network that is supposed to have Internet access, such as Admin.
2. On the Admin PC, open an Internet browser and attempt to access a website on the Internet such as http://www.fortinet.com.
   If this is successful, this PC has Internet access.
3. If step2 was not successful, at the command prompt on the PC enter `traceroute 22.11.22.33.`
   The output from this command should appear similar to:

```
Pinging 22.11.22.33 with 32 bytes of data:

Reply from 22.11.22.33: bytes=32 time<1m TTL=255
Reply from 22.11.22.33: bytes=32 time<1m TTL=255
Reply from 22.11.22.33: bytes=32 time<1m TTL=255
```

Advanced static routing example: ECMP failover and load balancing

Equal Cost Multi-Path (ECMP) load balancing and failover are methods that extend basic static routing. They allow you to use your network bandwidth more effectively and with less down time than if you used basic static routing alone.

The concepts in this section include:

- Equal-Cost Multi-Path (ECMP)
- Configuring interface status detection for gateway load balancing
- Configuring spillover or usage-based ECMP
- Configuring weighted static route load balancing

Equal-Cost Multi-Path (ECMP)

FortiOS uses equal-cost multi-path (ECMP) to distribute traffic to the same destination such as the Internet or another network. Using ECMP you can add multiple routes to the destination and give each of those routes the same distance and priority.

If multiple routes to the same destination have the same priority but different distances, the route with the lowest distance is used. If multiple routes to the same destination have the same distance but different priorities, the route with the lowest priority is used. Distance takes precedence over priority. If multiple routes to the same destination have different distances and different priorities, the route with the lowest distance is always used even if it has the highest priority.

If more than one ECMP route is available, you can configure how the FortiGate unit selects the route to be used for a communication session. If only one ECMP route is available (for example, because an interface cannot process traffic because interface status detection does not receive a reply from the configured server) then all traffic uses this route.

Previous versions of FortiOS provided source IP-based load balancing for ECMP routes, but now FortiOS includes three configuration options for ECMP route failover and load balancing:

Source IP based (also called source IP based)	The FortiGate unit load balances sessions among ECMP routes based on the source IP address of the sessions to be load balanced. This is the default load balancing method. No configuration changes are required to support source IP load balancing.
Weighted Load Balance (also called weight-based)	The FortiGate unit load balances sessions among ECMP routes based on weights added to ECMP routes. More traffic is directed to routes with higher weights. After selecting weight-based you must add weights to static routes.
Spillover (also called usage-based)	The FortiGate unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces added to the routes are. After selecting spill-over you add route Spillover Thresholds to interfaces added to ECMP routes. The FortiGate unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The FortiGate unit then spills additional sessions over to the next lowest numbered interface. The Spillover Thresholds range is 0-2097000 KBps.
Source-Destination IP based	The FortiGate unit load balances sessions among ECMP routes based on both the source and destination IP addresses of the sessions to be load balanced. This is required particularly for L3 link aggregation hashing.

You can configure only one of these ECMP route failover and load balancing methods in a single VDOM. If your FortiGate unit is configured for multiple VDOM operation, each VDOM can have its own ECMP route failover and load balancing configuration.

To configure the ECMP load balancing method from the web-based manager

1. Go to **Router > Static > Settings**.
2. Set **ECMP Load Balancing Method** to **Source IP based**, **Weighted Load Balance**, or **Spillover.**

To configure the ECMP load balancing method from the CLI

For example, to set the load balancing method to usage-based, enter the following:

```
config system settings
   set v4-ecmp-mode usage-based
end
```

ECMP routing of simultaneous sessions to the same destination IP address

When the FortiGate unit selects an ECMP route for a session, a route cache is created that matches the route with the destination IP address of the session. All new sessions to the same destination IP address from the same source IP address use the same route until the route is flushed from the cache. Routes are flushed from the cache after a period of time when no new sessions to the destination IP address are received.

The route cache improves FortiGate unit routing performance by reducing how often the FortiGate unit looks up routes in the routing table.

If the FortiGate unit receives a large number of sessions with the same destination IP address, because all of these sessions will be processed by the same route, it may appear that sessions are not distributed according to the ECMP route failover and load balancing configuration.

Configuring interface status detection for gateway load balancing

Interface status detection is used for ECMP route failover and load balancing. Interface status detection consists of the unit confirming that packets sent from an interface result in a response from a server. You can use up to three different protocols to confirm that an interface can connect to the server. Usually the server is the next-hop router that leads to an external network or the Internet. Interface status detection sends a packet using the configured protocols. If a response is received from the server, the unit assumes the interface can connect to the network. If a response is not received, the unit assumes that the interface cannot connect to the network.

Since it is possible that a response may not be received, even if the server and the network are operating normally, the dead gateway detection configuration controls the time interval between testing the connection to the server and the number of times the test can fail before the unit assumes that the interface cannot connect to the server.

As long as the unit receives responses for at least one of the protocols that you select, the unit assumes the server is operating and can forward packets. Responding to more than one protocol does not enhance the status of the server or interface.

To configure gateway failover detection for an interface - web-based manager

1. Go to **Router > Static > Settings**.
2. Under **Link Health Monitor**, select **Create New**.
3. Enter the following information:

Name	Give the monitor a name
Interface	Select the interface to test.
Gateway	Enter the IP address of the gateway.
Probe Type	Select the method of probe type, either Ping or HTTP.
Server	Address of Server to test. The address can be an IP address or FQDN. In some builds of the firmware if an invalid address is entered an error message comes up stating “Please enter an IP, IP range, FQDN, or comma separated list of IPs and/or FQDNs.” This is incorrect. Ranges cannot be used.
Probe Interval(s)	Enter the interval between pings, in seconds.
Failure Threshold	Enter the number of times the test can fail before the unit assumes that the interface cannot connect to the server.
Recovery Threshold	Configure the threshold for ECMP recovery, ranging from 1 to 10.
HA Priority	Set the HA priority, if configuring an HA cluster.

4. Select **OK**.

To configure gateway failover detection for an interface - CLI

```
config system link-monitor
   edit "test"
      set srcintf "internal4"
      set server "8.8.8.8"
      set update-cascade-interface disable
   end
```

Configuring spillover or usage-based ECMP

Spill-over or usage-based ECMP routes new sessions to interfaces that have not reached a configured bandwidth limit (called the **Spillover Threshold** or a route-spillover threshold). To configure spill-over or usage-based ECMP routing, you enable spill-over ECMP, add ECMP routes, and add a **Spillover Threshold** to the interfaces used by the ECMP routes. Set the **Spillover Thresholds** to limit the amount of bandwidth processed by each interface. The range is 0 to 2 097 000 Kbps. The threshold counts only outgoing traffic.

With spill-over ECMP routing configured, the FortiGate unit routes new sessions to an interface used by an ECMP route until that interface reaches its **Spillover Threshold**. Then, when the threshold of that interface is reached, new sessions are routed to one of the other interfaces used by the ECMP routes.

To add Spillover Thresholds to interfaces - web-based manager

Use the following steps to enable usage based ECMP routing, add Spillover Thresholds to FortiGate interfaces port3 and port4, and then to configure EMCP routes with device set to port3 and port4.

1. Go to **Router > Static > Settings**.
2. Set **ECMP Load Balance Method** to **Spillover**.

3. Go to **Router > Static > Static Route**s.
4. Add ECMP routes for `port3` and `port4`.

Destination IP/Mask	192.168.20.0/24
Device	port3
Gateway	172.20.130.3
Advanced	
Distance	10

Destination IP/Mask	192.168.20.0/24
Device	port4
Gateway	172.20.140.4
Advanced	
Distance	10

5. Go to **System > Network > Interfaces**.
6. Edit `port3` and `port4` and add the following spillover-thresholds:

Interface	port3
Spillover Threshold	100

Interface	port4
Spillover Threshold	200

To add Spillover Thresholds to interfaces - CLI

```
config system settings
   set v4-ecmp-mode usage-based
end
config router static
   edit 1
      set device port3
      set dst 192.168.20.0 255.255.255.0
      set gateway 172.20.130.3
   next
   edit 2
      set device port4
      set dst 192.168.20.0 255.255.255.0
      set gateway 172.20.140.4
   end
config system interface
```

```
edit port3
   set spillover-threshold 100
next
edit port4
   set spillover-threshold 200
end
```

Detailed description of how spill-over ECMP selects routes

When you add ECMP routes they are added to the routing table in the order displayed by the routing monitor or by the `get router info routing-table static` command. This order is independent of the configured bandwidth limit.

The FortiGate unit selects an ECMP route for a new session by finding the first route in the routing table that sends the session out a FortiGate unit interface that is not processing more traffic that its configured route spill-over limit.

A new session to a destination IP address that already has an entry in the routing cache is routed using the route already added to the cache for that destination address. See ECMP routing of simultaneous sessions to the same destination IP address on page 273.

For example, consider a FortiGate unit with interfaces port3 and port4 both connected to the Internet through different ISPs. ECMP routing is set to usage-based and route spillover for to 100 Kbps for port3 and 200 Kbps for port4. Two ECMP default routes are added, one for port3 and one for port4.

If the route to port3 is higher in the routing table than the route to port4, the FortiGate unit sends all default route sessions out port3 until port3 is processing 100Kbps of data. When port3 reaches its configured bandwidth limit, the FortiGate unit sends all default route sessions out port4. When the bandwidth usage of port3 falls below 100Kbps, the FortiGate again sends all default route sessions out port3.

New sessions with destination IP addresses that are already in the routing cache; however, use the cached routes. This means that even if port3 is exceeding its bandwidth limit, new sessions can continue to be sent out port3 if their destination addresses are already in the routing cache. As a result, new sessions are sent out port4 only if port3 exceeds its bandwidth limit and if the routing cache does not contain a route for the destination IP address of the new session.

Also, the switch over to port4 does not occur as soon as port3 exceeds its bandwidth limit. Bandwidth usage has to exceed the limit for a period of time before the switch over takes place. If port3 bandwidth usage drops below the bandwidth limit during this time period, sessions are not switched over to port4. This delay reduces route flapping.

FortiGate usage-based ECMP routing is not actually load balancing, since routes are not distributed evenly among FortiGate interfaces. Depending on traffic volumes, most traffic would usually be processed by the first interface with only spillover traffic being processed by other interfaces.

If you are configuring usage-based ECMP in most cases you should add spillover thresholds to all of the interfaces with ECMP routes. The default spillover threshold is 0 which means no bandwidth limiting. If any interface has a spillover threshold of 0, no sessions will be routed to interfaces lower in the list unless the interface goes down or is disconnected. An interface can go down if **Detect interface status for Gateway Load Balancing** does not receive a response from the configured server.

Determining if an interface has exceeded its Spillover Threshold

You can use the `diagnose netlink dstmac list` CLI command to determine if an interface is exceeding its Spillover Threshold. If the command displays **over_bps=1** the interface is exceeding its threshold. If **over_bps=0** the interface has not exceeded its threshold.

```
dev=Wifi mac=00:00:00:00:00:00 src-vis-os src-vis-host src-vis-user rx_tcp_
mss=0 tx_tcp_mss=0 overspill-threshold=0 bytes=0 over_bps=0 sampler_rate=0
```

Configuring weighted static route load balancing

Configure weighted load balancing to control how the FortiGate unit distributes sessions among ECMP routes by adding weights for each route. Add higher weights to routes that you want to load balance more sessions to.

With the ECMP load balancing method set to weighted, the FortiGate unit distributes sessions with different destination IPs by generating a random value to determine the route to select. The probability of selecting one route over another is based on the weight value of each route. Routes with higher weights are more likely to be selected.

Large numbers of sessions are evenly distributed among ECMP routes according to the route weight values. If all weights are the same, sessions are distributed evenly. The distribution of a small number of sessions; however, may not be even. For example, its possible that if there are two ECMP routes with the same weight; two sessions to different IP addresses could use the same route. On the other hand, 10,000 sessions with different destination IPs should be load balanced evenly between two routes with equal rates. The distribution could be 5000:5000 or 50001:4999. Also, 10 000 sessions with different destination IP addresses should be load balanced as 3333:6667 if the weights for the two routes are 100 and 200.

Weights only affect how routes are selected for sessions to new destination IP addresses. New sessions to IP addresses already in the routing cache are routed using the route for the session already in the cache. So in practice sessions will not always be distributed according to the routing weight distribution.

To add weights to static routes from the web-based manager

1. Go to **Router > Static > Settings**.
2. Set **ECMP Load Balance Method** to **Weighted Load Balance**.
3. Go to **Router > Static > Static Routes**.
4. If needed, add new static routes, for example:

Destination IP/Mask	192.168.20.0/24
Device	port1
Gateway	172.20.110.1
Distance	10

Destination IP/Mask	192.168.20.0/24
Device	port2

Gateway	172.20.120.2
Distance	10

5. Go to **Router > Static > Interfaces**.
6. Select a number next to an interface name, and choose **Edit** to change it, or simply double-click the interface name.
7. Set the weight; for example, set the weight of port1 to 100 and the weight of port2 to 200.

Dynamic Routing Overview

This section provides an overview of dynamic routing, and how it compares to static routing. For details on various dynamic routing protocols, see the following chapters for detailed information.

The following topics are included in this section:

What is dynamic routing?
Comparison of dynamic routing protocols
Choosing a routing protocol
Dynamic routing terminology
IPv6 in dynamic routing

What is dynamic routing?

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. Its this intelligent and hands-off approach that makes dynamic routing so useful.

Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors. For more information on these administrative distances, see Advanced Static Routing on page 242.

This section includes:

- Comparing static and dynamic routing
- Dynamic routing protocols
- Minimum configuration for dynamic routing

Comparing static and dynamic routing

A common term used to describe dynamic routing is convergence. Convergence is the ability to work around network problems and outages — for the routing to come together despite obstacles. For example, if the main router between two end points goes down, convergence is the ability to find a way around that failed router and reach the destination. Static routing has zero convergence beyond trying the next route in its limited local routing table — if a network administrator doesn't fix a routing problem manually, it may never be fixed, resulting in a downed network. Dynamic routing solves this problem by involving routers along the route in the decision-making about the optimal route, and using the routing tables of these routers for potential routes around the outage. In general, dynamic routing has better scalability, robustness, and convergence. However, the cost of these added benefits include more complexity and some overhead: the routing protocol uses some bandwidth for its own administration.

Comparing static and dynamic routing

Feature	Static Routing	Dynamic Routing
Hardware support	Supported by all routing hardware	May require special, more expensive routers
Router Memory Required	Minimal	Can require considerable memory for larger tables
Complexity	Simple	Complex
Overhead	None	Varying amounts of bandwidth used for routing protocol updates
Scalability	Limited to small networks	Very scalable, better for larger networks
Robustness	None - if a route fails it has to be fixed manually	Robust - traffic routed around failures automatically
Convergence	None	Varies from good to excellent

Dynamic routing protocols

A dynamic routing protocol is an agreed-on method of routing that the sender, receiver, and all routers along the path (route) support. Typically the routing protocol involves a process running on all computers and routers along that route to enable each router to handle routes in the same way as the others. The routing protocol determines how the routing tables are populated along that route, how the data is formatted for transmission, and what information about a route is included with that route. For example RIP, and BGP use distance vector algorithms, where OSPF uses a shortest path first algorithm. Each routing protocol has different strengths and weaknesses — one protocol may have fast convergence, while another may be very reliable, and a third is very popular for certain businesses like Internet Service Providers (ISPs).

Dynamic routing protocols are different from each other in a number of ways, such as:

- Classful versus classless routing protocols
- Interior versus exterior routing protocols
- Distance vector versus link-state protocols

Classful versus classless routing protocols

Classful or classless routing refers to how the routing protocol handes the IP addresses. In classful addresses there is the specific address, and the host address of the server that address is connected to. Classless addresses use a combination of IP address and netmask.

Classless Inter-Domain Routing (CIDR) was introduced in 1993 (originally with RFC 1519 and most recently with RFC 4632) to keep routing tables from getting too large. With Classful routing, each IP address requires its own entry in the routing table. With Classless routing, a series of addresses can be combined into one entry potentially saving vast amounts of space in routing tables.

Current routing protocols that support classless routing out of necessity include RIPv2, BGP, IS-IS, and OSPF. Older protocols such as RIPv1 do not support CIDR addresses.

Interior versus exterior routing protocols

The names ***interior*** and ***exterior*** are very descriptive. Interior routing protocols are designed for use within a contained network of limited size, whereas exterior routing protocols are designed to link multiple networks together. They can be used in combination in order to simplify network administration. For example, a network can be built with only border routers of a network running the exterior routing protocol, while all the routers on the network run the interior protocol, which prevents them from connecting outside the network without passing through the border. Exterior routers in such a configuration must have both exterior and interior protocols, to communicate with the interior routers and outside the network.

Nearly all routing protocols are interior routing protocols. Only BGP is commonly used as an exterior routing protocol.

You may see interior gateway protocol (IGP) used to refer to interior routing protocols, and exterior gateway protocol (EGP) used to refer to interior routing protocols.

Distance vector versus link-state protocols

Every routing protocol determines the best route between two addresses using a different method. However, there are two main algorithms for determining the best route — Distance vector and Link-state.

Distance vector protocols

In distance vector protocols, routers are told about remote networks through neighboring routers. The distance part refers to the number of hops to the destination, and in more advanced routing protocols these hops can be weighted by factors such as available bandwidth and delay. The vector part determines which router is the next step along the path for this route. This information is passed along from neighboring routers with routing update packets that keep the routing tables up to date. Using this method, an outage along a route is reported back along to the start of that route, ideally before the outage is encountered.

On distance vector protocols, RFC 1058 which defines RIP v1 states the following:

> *Distance vector algorithms are based on the exchange of only a small amount of information. Each entity (gateway or host) that participates in the routing protocol is assumed to keep information about all of the destinations within the system. Generally, information about all entities connected to one network is summarized by a single entry, which describes the route to all destinations on that network.*

There are four main weaknesses inherent in the distance vector method. Firstly, the routing information is not discovered by the router itself, but is instead reported information that must be relied on to be accurate and up-to-date. The second weakness is that it can take a while for the information to make its way to all the routers who need the information — in other words it can have slow convergence. The third weakness is the amount of overhead involved in passing these updates all the time. The number of updates between routers in a larger network can significantly reduce the available bandwidth. The fourth weakness is that distance vector protocols can end up with routing-loops. Routing loops are when packets are routed for ever around a network, and often occur with slow convergence. The bandwidth required by these infinite loops will slow your network to a halt. There are methods of preventing these loops however, so this weakness is not as serious as it may first appear.

Link-state protocols

Link-state protocols are also known as shortest path first protocols. Where distance vector uses information passed along that may or may not be current and accurate, in link-state protocols each router passes along only information about networks and devices directly connected to it. This results in a more accurate picture of the network topology around your router, allowing it to make better routing decisions. This information is passed between routers using link-state advertisements (LSAs). To reduce the overhead, LSAs are only sent out when information changes, compared to distance vector sending updates at regular intervals even if no information has changed. The more accurate network picture in link-state protocols greatly speed up convergence and avoid problems such as routing-loops.

Minimum configuration for dynamic routing

Dynamic routing protocols do not pay attention to routing updates from other sources, unless you specifically configure them to do so using CLI redistribute commands within each routing protocol.

The minimum configuration for any dynamic routing to function is to have dynamic routing configured on one interface on the FortiGate unit, and one other router configured as well. Some protocols require larger networks to function as designed.

Minimum configuration based on dynamic protocol

	BGP	RIP	OSPF / IS-IS
Interface	yes	yes	yes
Network	yes	yes	yes
AS	local and neighbor	no	yes
Neighbors	at least one	at least one	at least one
Version	no	yes	no
Router ID	no	no	yes

Comparison of dynamic routing protocols

Each dynamic routing protocol was designed to meet a specific routing need. Each protocol does some things well, and other things not so well. For this reason, choosing the right dynamic routing protocol for your situation is not an easy task.

Features of dynamic routing protocols

Each protocol is better suited for some situations over others.

Choosing the best dynamic routing protocol depends on the size of your network, speed of convergence required, the level of network maintenance resources available, what protocols the networks you connect to are using, and so on. For more information on these dynamic routing protocols, see Routing Information Protocol (RIP) on page 295, Border Gateway Protocol (BGP) on page 332, Open Shortest Path First (OSPF) on page 371, and Intermediate System to Intermediate System Protocol(IS-IS) on page 412.

Comparing RIP, BGP, and OSPF dynamic routing protocols

Protocol	RIP	BGP	OSPF / IS-IS
Routing algorithm	Distance Vector, basic	Distance Vector, advanced	Link-state
Common uses	Small non-complex networks	Network backbone, ties multinational offices together	Common in large, complex enterprise networks
Strengths	Fast and simple to implement Near universal support Good when no redundant paths	Graceful restart BFD support Only needed on border routers Summarize routes	Fast convergence Robust Little management overhead No hop count limitation Scalable
Weakness	Frequent updates can flood network Slow convergence Maximum 15 hops may limit network configuration	Required full mesh in large networks can cause floods Route flap Load-balance multihomed networks Not available on low-end routers	Complex No support for unequal cost multipath routing Route summary can require network changes
Authentication	Optional authentication using text string or MD5 password. (RIP v1 has no authentication)		
IPv6 Support	Only in RIPng	Only in BGP4+	Only in OSPF6 / Integrated IS-IS

Routing protocols

- ***Routing Information Protocol (RIP)*** uses classful routing, as well as incorporating various methods to stop incorrect route information from propagating, such as the poisoned horizon method. However, on larger networks its frequent updates can flood the network and its slow convergence can be a problem.
- ***Border Gateway Protocol (BGP)*** has been the core Internet backbone routing protocol since the mid 1990s, and is the most used interior gateway protocol (IGP). However, some configurations require full mesh connections which flood the network, and there can be route flap and load balancing issues for multihomed networks.
- ***Open Shortest Path First (OSPF)*** is commonly used in large enterprise networks. It is the protocol of choice mainly due to its fast convergence. However, it can be complicated to setup properly.

- ***Intermediate System to Intermediate System (IS-IS) Protocol*** allows routing of ISO's OSI protocol stack Connectionless Network Service (CLNS). IS-IS is an Interior Gateway Protocol (IGP) not intended to be used between Autonomous Systems (ASes). IS-IS is a link state protocol well-suited to smaller networks that is in widespread use and has near universal support on routing hardware.
- ***Multicast*** addressing is used to broadcast from one source to many destinations efficiently. Protocol Independent Multicast (PIM) is the protocol commonly used in enterprises, multimedia content delivery, and stock exchanges.

Routing algorithm

Each protocol uses a slightly different algorithm for choosing the best route between two addresses on the network. The algorithm is the "intelligent" part of a dynamic protocol because the algorithm is responsible for deciding which route is best and should be added to the local routing table. RIP and BGP use distance vector algorithms, where OSPF and IS-IS use link-state or a shortest path first algorithm.

Vector algorithms are essentially based on the number of hops between the originator and the destination in a route, possibly weighting hops based on how reliable, fast, and error-free they are.

The link-state algorithm used by OSPF and IS-IS is called the Dijkstra algorithm. Link-state treats each interface as a link, and records information about the state of the interface. The Dijkstra algorithm creates trees to find the shortest paths to the routes it needs based on the total cost of the parts of the routes in the tree.

For more information on the routing algorithm used, see Comparison of dynamic routing protocols on page 282.

Authentication

If an attacker gains access to your network, they can masquerade as a router on your network to either gain information about your network or disrupt network traffic. If you have a high quality firewall configured, it will help your network security and stop many of this type of threat. However, the main method for protecting your routing information is to use authentication in your routing protocol. Using authentication on your FortiGate unit and other routers prevents access by attackers — all routers must authenticate with passwords, such as MD5 hash passwords, to ensure they are legitimate routers.

When configuring authentication on your network, ensure you configure it the same on all devices on the network. Failure to do so will create errors and outages as those forgotten devices fail to connect to the rest of the network.

For example, to configure an MD5 key of `123` on an OSPF interface called `ospf_test`, enter the following CLI command:

```
config router ospf
   config ospf-interface
      edit ospf_test
         set authentication md5
         set md5-key 123
      end
   end
```

Convergence

Convergence is the ability of a networking protocol to re-route around network outages. Static routing cannot do this. Dynamic routing protocols can all converge, but take various amounts of time to do this. Slow convergence can cause problems such as network loops which degrade network performance.

You may also hear robustness and redundancy used to describe networking protocols. In many ways they are the same thing as convergence. Robustness is the ability to keep working even though there are problems, including

configuration problems as well as network outages. Redundancy involves having duplicate parts that can continue to function in the event of some malfunction, error, or outage. It is relatively easy to configure dynamic routing protocols to have backup routers and configurations that will continue to function no matter the network problem short of a total network failure.

IPv6 Support

IPv4 addressing is in common use everywhere around the world. IPv6 has much larger addresses and it is used by many large companies and government departments. IPv6 is not as common as IPv4 yet, but more companies are adopting it.

If your network uses IPv6, your dynamic routing protocol must support it. None of the dynamic routing protocols originally supported IPv6, but they all have additions, expansions, or new versions that do support IPv6. For more information, see Routing Information Protocol (RIP) on page 295, Border Gateway Protocol (BGP) on page 332, Open Shortest Path First (OSPF) on page 371, or Intermediate System to Intermediate System Protocol(IS-IS) on page 412.

When to adopt dynamic routing

Static routing is more than enough to meet your networking needs when you have a small network. However, as your network grows, the question you need to answer is at what point do you adopt dynamic routing in your networking plan and start using it in your network? The main factors in this decision are typically:

- Budget
- Current network size and topology
- Expected network growth
- Available resources for ongoing maintenance

Budget

When making any business decision, the budget must always be considered. Static routing does not involve special hardware, fancy software, or expensive training courses.

Dynamic routing can include all of these extra expenses. Any new hardware, such as routers and switches, will need to support your chosen routing protocols. Network management software and routing protocol drivers may be necessary as well to help configure and maintain your more complex network. If the network administrators are not well versed in dynamic routing, either a training course or some hands-on learning time must be budgeted so they can administer the new network with confidence. Together, these factors can impact your budget.

Additionally, people will always account for network starting costs in the budgets, but usually leave out the ongoing cost of network maintenance. Any budget must provide for the hours that will be spent on updating the network routing equipment, and fixing any problems. Without that money in the budget, you may end up back at static routing before you know it.

Current network size and topology

As stated earlier static routing works well on small networks. At those networks get larger, routing takes longer, routing tables get very large, and general performance isn't what it could be.

Topology is a concern as well. If all your computers are in one building, its much easier to stay with static routing longer. However, connecting a number of locations will be easier with the move to dynamic routing.

If you have a network of 20 computers, you can still likely use static routing. If those computers are in two or three locations, static routing will still be a good choice for connecting them. Also, if you just connect to your ISP and don't worry about any special routing to do that, you are likely safe with just static routing.

If you have a network of 100 computers in one location, you can use static routing but it will be getting slower, more complex, and there won't be much room for expansion. If those 100 computers are spread across three or more locations, dynamic routing is the way to go.

If you have 1000 computers, you definitely need to use dynamic routing no matter how many locations you have.

Hopefully this section has given you an idea of what results you will likely experience from different sized networks using different routing protocols. Your choice of which dynamic routing protocol to use is partly determined by the network size, and topology.

Expected network growth

You may not be sure if your current network is ready for dynamic routing. However, if you are expecting rapid growth in the near future, it is a good idea to start planning for that growth now so you are ready for the coming expansion.

Static routing is very labor intensive. Each network device's routing table needs to be configured and maintained manually. If there is a large number of new computers being added to the network, they each need to have the static routing table configured and maintained. If devices are being moved around the network frequently, they must also be updated each time.

Instead, consider putting dynamic routing in place before those new computers are installed on the network. The installation issues can be worked out with a smaller and less complex network, and when those new computers or routers are added to the network there will be nowhere near the level of manual configuration required. Depending on the level of growth, this labor savings can be significant. For example, in an emergency you can drop a new router into a network or AS, wait for it to receive the routing updates from its neighbors, and then remove one of the neighbors. While the routes will not be the most effective possible, this method is much less work than static routing in the same situation, with less chance of mistakes.

Also, as your network grows and you add more routers, those new routers can help share the load in most dynamic routing configurations. For example if you have 4 OSPF routers and 20,000 external routes those few routers will be overwhelmed. But in a network with 15 OSPF routers they will better be able to handle that number of routes. Be aware though that adding more routers to your network will increase the amount of updates sent between the routers, which will use up a greater part of your bandwidth and use more bandwidth overall.

Available resources for ongoing maintenance

As touched on in the budget section, there must be resources dedicated to ongoing network maintenance, upgrades, and troubleshooting. These resources include administrator hours to configure and maintain the network, training for the administrator if needed, extra hardware and software as needed, and possible extra staff to help the administrator in emergencies. Without these resources, you will quickly find the network reverting to static routing out of necessity. This is because:

- Routing software updates will require time.
- Routing hardware updates will require time.
- Office reorganizations or significant personnel movement will require time from a networking point of view.
- Networking problems that occur, such as failed hardware, require time to locate and fix the problem.

If the resources to accomplish these tasks are not budgeted, they will either not happen or not happen at the required level to continue operation. This will result in both the network administration staff and the network users being very frustrated.

A lack of maintenance budget will also result in increasingly heavy reliance on static routing as the network administrators are forced to use quick fixes for problems that come up. This invariably involves going to static routing, and dropping the more complex and time-consuming dynamic routing.

Choosing a routing protocol

One of that hardest decisions in routing can be choosing which routing protocol to use on your network. It can be easy to decide when static routing will not meet your needs, but how can you tell which dynamic routing protocol is best for your network and situation?

Here is a brief look at the routing protocols including their strongest and weakest points. The steps to choosing your routing protocol are:

1. Answer questions about your network
2. Evaluate your chosen protocol
3. Implement your dynamic routing protocol

Answer questions about your network

Before you can decide what is best for your situation, you need to examine what the details of your situation are such as what you have for budget, equipment, and users.

The following questions will help you form a clear idea of your routing needs:

How many computers or devices are on your network?

It matters if you only have a few computers, or if you have many and if they are all at one location or not as well. All routing protocols can be run on any sized network, however it can be inefficient to run some on very small networks. However, routers and network hardware that support dynamic routing can be more expensive than more generic routers for static routing.

What applications typically run over the network?

Finding out what application your users are running will help you determine their needs and the needs of the network regarding bandwidth, quality of service, and other such issues.

What level of service do the users expect from the network?

Different network users have different expectations of the network. Its not critical for someone surfing the Internet to have 100% uptime, but it is required for a stock exchange network or a hospital.

Is there network expansion in your near future?

You may have a small network now, but if it will be growing quickly, you should plan for the expected size so you don’t have to chance technologies again down the road.

What routing protocols do your networks connect to?

This is most often how routing protocol decisions are made. You need to be able to communicate easily with your service provider and neighbors, so often people simply use what everyone else is using.

Is security a major concern?

Some routing protocols have levels of authentication and other security features built in. Others do not. If security is important to you, be aware of this.

What is your budget — both initial and maintenance?

More robust and feature laden routing protocols generally mean more resources are required to keep them working well. Also more secure configurations require still more resources. This includes both set up costs, as well as ongoing maintenance costs. Ignore these costs at the risk of having to drop the adoption of the new routing protocol mid-change.

Evaluate your chosen protocol

Once you have examined the features of the routing protocols listed above and chosen the one that best meets your needs, you can set up an evaluation or test install of that protocol.

The test install is generally set up in a sandbox configuration so it will not affect critical network traffic. The aim of the test install is to prove that it will work on a larger scale on your network. So be sure that the test install mirrors your larger network well enough for you to discover any problems. If its too simplistic, these problems may not appear.

If your chosen protocol does not meet your goals choose a different protocol and repeat the evaluation process until either a protocol meets your needs, or you change your criteria.

Implement your dynamic routing protocol

You have examined your needs, selected the best matching dynamic routing protocol, tested it, and now you are ready to implement it with confidence.

This guide will help you configure your FortiGate unit to support your chosen dynamic routing protocol. Refer to the various sections in this guide as needed during your implementation to help ensure a smooth transition. Examples for each protocol have been included to show proper configurations for different types of networks.

Dynamic routing terminology

Dynamic routing is a complex subject. There are many routers on different networks and all can be configured differently. It become even more complicated when you add to this each routing protocol having slightly different names for similar features, and many configurable features for each protocol.

To better understand dynamic routing, here are some explanations of common dynamic routing terms.

- Aggregated routes and addresses
- Autonomous system (AS)
- Area border router (ABR)
- Neighbor routers
- Route maps

- Access lists
- Bi-directional forwarding detection (BFD)

For more details on a term as it applies to a dynamic routing protocol, see one of Border Gateway Protocol (BGP) on page 332, Routing Information Protocol (RIP) on page 295, or Open Shortest Path First (OSPF) on page 371.

Aggregated routes and addresses

Just as an aggregate interface combines multiple interfaces into one virtual interface, an aggregate route combines multiple routes into one. This reduces the amount of space those routes require in the routing tables of the routers along that route. The trade-off is a small amount of processing to aggregate and de-aggregate the routes at either end.

The benefit of this method is that you can combine many addresses into one, potentially reducing the routing table size immensely. The weakness of this method is if there are holes in the address range you are aggregating you need to decide if its better to break it into multiple ranges, or accept the possibility of failed routes to the missing addresses.

For information on aggregated routes in BGP, see Border Gateway Protocol (BGP) on page 332, and Border Gateway Protocol (BGP) on page 332.

To manually aggregate the range of IP addresses from 192.168.1.100 to 192.168.1.103

1. Convert the addresses to binary
   ```
   192.168.1.100 = 11000000 10101000 00000001 01100100
   192.168.1.101 = 11000000 10101000 00000001 01100101
   192.168.1.102 = 11000000 10101000 00000001 01100110
   192.168.1.103 = 11000000 10101000 00000001 01100111
   ```
2. Determine the maximum number of matching bits common to the addresses.
   There are 30-bits in common, with only the last 2-bits being different.
3. Record the common part of the address.
   ```
   11000000 10101000 00000001 0110010X = 192.168.1.100
   ```
4. For the netmask, assume all the bits in the netmask are 1 except those that are different which are 0.
   ```
   11111111 11111111 11111111 11111100 = 255.255.255.252
   ```
5. Combine the common address bits and the netmask.
   ```
   192.168.1.100/255.255.255.252
   ```
   Alternately the IP mask may be written as a single number:
   ```
   192.168.1.100/30
   ```
6. As required, set variables and attributes to declare the routes have been aggregated, and what router did the aggregating.

Autonomous system (AS)

An Autonomous System (AS) is one or more connected networks that use the same routing protocol, and appear to be a single unit to any externally connected networks. For example an ISP may have a number of customer networks connected to it, but to any networks connected externally to the ISP it appears as one system or AS. An AS may also be referred to as a routing domain.

It should be noted that while OSPF routing takes place within one AS, the only part of OSPF that deals with the AS is the AS border router (ASBR).

There are multiple types of AS defined by how they are connected to other ASes. A multihomed AS is connected to at least two other ASes and has the benefit of redundancy — if one of those ASes goes down, your AS can still reach the Internet through its other connection. A stub AS only has one connection, and can be useful in specific configurations where limited access is desirable.

Each AS has a number assigned to it, known as an ASN. In an internal network, you can assign any ASN you like (a private AS number), but for networks connected to the Internet (public AS) you need to have an officially registered ASN from Internet Assigned Numbers Authority (IANA). ASNs from 1 to 64,511 are designated for public use.

NAs of January 2010, AS numbers are 4 bytes long instead of the former 2 bytes. RFC 4893 introduced 32-bit ASNs, which FortiGate units support for BGP and OSPF.

Do you need your own AS?

The main factors in deciding if you need your own AS or if you should be part of someone else's are:

- exchanging external routing information
- many prefixes should exist in one AS as long as they use the same routing policy
- when you use a different routing protocol than your border gateway peers (for example your ISP uses BGP, and you use OSPF)
- connected to multiple other AS (multi-homed)

You should not create an AS for each prefix on your network. Neither should you be forced into an AS just so someone else can make AS-based policy decisions on your traffic.

There can be only one AS for any prefix on the Internet. This is to prevent routing issues.

What AS number to use?

In addition to overseeing IP address allocation and Domain Name Systems (DNS), the Internet Assigned Numbers Authority (IANA) assigns public AS numbers. The public AS numbers are from 1 to 64,511. The ASNs 0, 54272–64511, and 65535 are reserved by the IANA. These ASNs should not be used.

ASNs are assigned in blocks by the Internet Assigned Numbers Authority (IANA) to Regional Internet Registries (RIRs) who then assign ASNs to companies within that RIRs geographic area. Usually these companies are ISPs, and to receive an ASN you must complete the application process of the local RIR and be approved before being assigned an ASN. The RIRs names and regions are:

AFRINIC	Serves the African continent
APNIC	Asia-Pacific including China, India, and Japan
ARIN	American registry including Canada and United States
LACNIC	Latin America, including Mexico, Caribbean, Central and South America
RIPE NCC	Europe, the Middle East, former USSR, and parts of Central Asia

AS numbers from 64512 to 65534 are reserved for private use. Private AS numbers can be used for any internal networks with no outside connections to the Internet such as test networks, classroom labs, or other internal-only networks that do not access the outside world. You can also configure border routers to filter out any private ASNs before routing traffic to the outside world. If you must use private ASNs with public networks, this is the only way to configure them. However, it is risky because many other private networks could be using the same ASNs and conflicts will happen. It would be very much like your local 192.168.0.0 network being made public — the resulting problems would be widespread.

In 1996, when RFC 1930 was written only 5,100 ASes had been allocated and a little under 600 ASes were actively routed in the global Internet. Since that time many more public ASNs have been assigned, leaving only a small number. For this reason 32-bit ASNs (four-octet ASNs) were defined to provide more public ASNs. RFC 4893 defines 32-bit ASNs, and FortiGate units support these larger ASNs.

Area border router (ABR)

Routers within an AS advertise updates internally and only to each other. However, routers on the edge of the AS must communicate both with routers inside their AS and with routers external to their AS, often running a different routing protocol. These routers are called Area Border Routers (ABRs) or edge routers. Often ABRs run multiple routing protocols to be able to redistribute traffic between different ASes that are running different protocols, such as the edge between an ISP's IS-IS routing network and a large company's OSPF network.

OSPF defines ABRs differently from other routers. In OSPF, an ABR is an OSPF router that connects another AS to the backbone AS, and is a member of all the areas it connects to. An OSPF ABR maintains a LSA database for each area that it is connected to. The concept of the edge router is present, but its the edge of the backbone instead of the edge of the OSPF supported ASes.

Neighbor routers

Routing involves routers communicating with each other. To do this, routers need to know information about each other. These routers are called neighbor routers, and are configured in each routing protocol. Each neighbor has custom settings since some routers may have functionality others routers lack. Neighbor routers are sometimes called peers.

Generally neighbor routers must be configured, and discovered by the rest of the network before they can be integrated to the routing calculations. This is a combination of the network administrator configuring the new router with its neighbor router addresses, and the routing network discovering the new router, such as the hello packets in OSPF. That discovery initiates communication between the new router and the rest of the network.

Route maps

Route maps are a way for the FortiGate unit to evaluate optimum routes for forwarding packets or suppressing the routing of packets to particular destinations. Compared to access lists, route maps support enhanced packet-matching criteria. In addition, route maps can be configured to permit or deny the addition of routes to the FortiGate unit routing table and make changes to routing information dynamically as defined through route-map rules.

Route maps can be used for limiting both received route updates, and sent route updates. This can include the redistribution of routes learned from other types of routing. For example if you don't want to advertise local static routes to external networks, you could use a route map to accomplish this.

The FortiGate unit compares the rules in a route map to the attributes of a route. The rules are examined in ascending order until one or more of the rules in the route map are found to match one or more of the route attributes.

As an administrator, route maps allow you to group a set of addresses together and assign them a meaningful name. Then during your configuration, you can use these route-maps to speed up configuration. The meaningful names ensure fewer mistakes during configuration as well.

The default rule in the route map (which the FortiGate unit applies last) denies all routes. For a route map to take effect, it must be called by a FortiGate unit routing process.

The syntax for route maps are:

```
config router route-map
   edit <route_map_name>
      set comments
      config rule
         edit <route_map_rule_id>
            set action
            set match-*
            set set-*
            ...
         end
```

The `match-*` commands allow you to match various parts of a route. The `set-*` commands allow you to set routing information once a route is matched.

For an example of how route maps can be used to create receiving or sending “groups” in routing, see Border Gateway Protocol (BGP) on page 332.

Access lists

Use this command to add, edit, or delete access lists. Access lists are filters used by FortiGate unit routing processes. For an access list to take effect, it must be called by a FortiGate unit routing process (for example, a process that supports RIP or OSPF). Use `access-list6` for IPv6 routing.

Access lists can be used to filter which updates are passed between routers, or which routes are redistributed to different networks and routing protocols. You can create lists of rules that will match all routes for a specific router or group of routers.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route, 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose.

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

The syntax for access lists is:

```
config router access-list, access-list6
   edit <access_list_name>
      set comments
      config rule
```

```
edit <access_list_id>
   set action
   set exact-match
   set prefix
   set prefix6
   set wildcard
```

For an example of how access lists can be used to create receiving or sending “groups” in routing, see Border Gateway Protocol (BGP) on page 332.

Bi-directional forwarding detection (BFD)

Bi-directional Forwarding Detection (BFD) is a protocol used to quickly locate hardware failures in the network. Routers running BFD send packets to each other at a negotiated rate. If packets from a BFD-protected router fail to arrive, then that router is declared down. BFD communicates this information to the routing protocol and the routing information is updated.

BFD neighbors establish if BFD is enabled in OSPF or BFP routers that establish as neighbors.

The CLI commands associated with BFD include:

```
config router bgp
   config neighbor
      set bfd
end
config router ospf
   set bfd
end
```

Per-VDOM configuration:

```
config system settings
   set bfd
   set bfd-desired-min-tx
   set bfd-required-min-rx
   set bfd-detect-mult
   set bfd-dont-enforce-src-port
end
```

Per-interface (override) configuration:

```
config system interface
   edit <interface_name>
      set bfd enable
      set bfd-desired-min-tx
      set bfd-detect-mult
      set bfd-required-min-rx
   end
```

For more information about BFD in BGP, see Border Gateway Protocol (BGP) on page 332.

IPv6 in dynamic routing

Unless otherwise stated, routing protocols apply to IPv4 addressing. This is the standard address format used. However, IPv6 is becoming more popular and new versions of the dynamic routing protocols have been introduced.

Dynamic routing supports IPv6 on your FortiGate unit. The new versions of these protocols and the corresponding RFCs are:

- **RIP next generation (RIPng)** — RFC 2080 - Routing Information Protocol next generation (RIPng). See RIP and IPv6.
- **BGP4+** — RFC 2545, and RFC 2858 Multiprotocol Extensions for IPv6 Inter-Domain Routing, and Multiprotocol Extensions for BGP-4 (MP-BGP) respectively. See BGP and IPv6.
- **OSPFv3** — RFC 2740 Open Shortest Path First version 3 (OSPFv3) for IPv6 support. See OSPFv3 and IPv6.
- **Integrated IS-IS** — RFC 5308 for IPv6 support. See Integrated IS-IS.

As with most advanced routing features on your FortiGate unit, IPv6 settings for dynamic routing protocols must be enabled before they will be visible in the GUI. To enable IPv6 configuration in the GUI, enable it in **System > Admin > Settings**. Alternatively, you can directly configure IPv6 for RIP, BGP, or OSPF protocols using CLI commands.

Routing Information Protocol (RIP)

This section describes the Routing Information Protocol (RIP).

The following topics are included in this section:

RIP background and concepts
Troubleshooting RIP
Simple RIP example
RIPng — RIP and IPv6

RIP background and concepts

This section contains:

- Background
- Parts and terminology of RIP
- How RIP works

Background

Routing Information Protocol (RIP) is a distance-vector routing protocol intended for small, relatively homogeneous networks. Its widespread use started when an early version of RIP was included with BSD v4.3 Linux as the routed daemon. The routing algorithm used by RIP, the Bellman–Ford algorithm, first saw widespread use as the initial routing algorithm of the ARPANET.

RIP benefits include being well suited to smaller networks, is in widespread use, near universal support on routing hardware, quick to configure, and works well if there are no redundant paths. However, RIP updates are sent out node-by-node so it can be slow to find a path around network outages. RIP also lacks good authentication, can not choose routes based on different quality of service methods, and can create network loops if you are not careful.

The FortiGate implementation of RIP supports RIP version 1 (see RFC 1058), RIP version 2 (see RFC 2453), and the IPv6 version RIPng (see RFC 2080).

RIP v1

In 1988 RIP version 1, defined in RFC 1058, was released. The RFC even states that RIP v1 is based on Linux routed due to it being a “defacto standard”.

It uses classful addressing and uses broadcasting to send out updates to router neighbors. There is no subnet information included in the routing updates in classful routing, and it does not support CIDR addressing — subnets must all be the same size. Also, route summarization is not possible.

RIP v1 has no router authentication method, so it is vulnerable to attacks through packet sniffing, and spoofing.

RIP v2

In 1993, RIP version 2 was developed to deal with the limitations of RIP v1. It was not standardized until 1998. This new version supports classless routing, and subnets of various sizes.

Router authentication was added in RIP v2 — it supports MD5. MD5 hashes are an older encryption method, but this is much improved over no security at all.

In RIP v2 the hop count limit remained at 15 to be backwards compatible with RIP v1.

RIP v2 uses multicasting to send the entire routing table to router neighbors, thereby reducing the traffic for devices that are not participating in RIP routing.

Routing tags were added as well, which allow internal routes or redistributed routes to be identified as such.

RIPng

RIPng, defined in RFC 2080, is an extension of RIP2 designed to support IPv6. However, RIPng varies from RIPv2 in that it is not fully backwards compatible with RIPv1.

- RIPng does not support RIPv1 update authentication, it relies on IPsec
- RIPng does not allow attaching tags to routes as in RIPv2
- RIPng requires specific encoding of the next hop for a set of route entries, unlike RIPv2 that encodes the next-hop into each route entry.

Parts and terminology of RIP

Before you can understand how RIP functions, you need to understand some of the main concepts and parts of RIP.

This section includes:

- RIP and IPv6
- Default information originate option
- Update, Timeout, and Garbage timers
- Authentication and key-chain
- Access Lists

RIP and IPv6

RIP Next Generation (RIPng) is a new version of RIP was released that includes support for IPv6.

The FortiGate unit command `config router ripng` is almost the same as `config router rip`, except that IPv6 addresses are used. Also if you are going to use prefix or access lists with RIPng, you must use the `config router access-list6` or `config prefix-list6` versions of those commands.

If you want to troubleshoot RIPng, it is the same as with RIP but specify the different protocol, and use IPv6 addresses. This applies to commands such as `get router info6` when you want to see the routing table, or other related information.

If you want to route IPv4 traffic over an IPv6 network, you can use the command `config system ip6-tunnel` to configure the FortiGate unit to do this. The IPv6 interface is configured under `config system interface`. All subnets between the source and destination addresses must support IPv6. This command is not supported in Transparent mode.

For example, you want to set up a tunnel on the port1 interface starting at 2002:C0A8:3201:: on your local network and tunnel it to address 2002:A0A:A01:: where it will need access to an IPv4 network again. Use the following command:

```
config system ipv6-tunnel
```

```
    edit test_tunnel
      set destination 2002:A0A:A01::
      set interface port1
      set source 2002:C0A8:3201::
    end
end
```

The CLI commands associated with RIPng include:

```
config router ripng
config router access-list6
config router prefix-list6
config system ipv6-tunnel
get router info6 *
```

Default information originate option

This is the second advanced option for RIP in the web-based manager, right after metric. Enabling default-information-originate will generate and advertise a default route into the FortiGate unit's RIP-enabled networks. The generated route may be based on routes learned through a dynamic routing protocol, routes in the routing table, or both. RIP does not create the default route unless you use the always option.

Select **Disable** if you experience any issues or if you wish to advertise your own static routes into RIP updates.

You can enable or disable default-information-originate in **Router > Dynamic > RIP**, under **Advanced Options**, or use the CLI.

The CLI commands associated with default information originate include:

```
config router rip
   set default-information-originate
end
```

Update, Timeout, and Garbage timers

RIP uses various timers to regulate its performance including an update timer, a timeout timer, and a garbage timer. The FortiGate unit default timer settings (30, 180, and 120 seconds respectively) are effective in most configurations — if you change these settings, ensure that the new settings are compatible with local routers and access servers.

The Timeout period should be at least three times longer than the Update period. If the Update timer is smaller than Timeout or Garbage timers, you will experience an error.

You can set the three RIP timers in **Router > Dynamic > RIP**, under **Advanced Options**, or use the CLI.

The CLI commands associated with garbage, timeout, and update timers include:

```
config router rip
   set timeout-timer
   set update-timer
   set garbage-timer
end
```

Update timer

The update timer determines the interval between routing updates. Generally, this value is set to 30 seconds. There is some randomness added to help prevent network traffic congestion, which could result from all routers simultaneously attempting to update their neighbors. The update timer should be at least three times smaller than the timeout timer, otherwise you will experience an error.

If you are experiencing significant RIP traffic on your network, you can increase this interval to send fewer updates per minute. However, ensure you increase the interval for all the routers on your network or you will experience time outs that will degrade your network speed.

Timeout timer

The timeout timer is the maximum amount of time (in seconds) that a route is considered reachable while no updates are received for the route. This is the maximum time the FortiGate unit will keep a reachable route in the routing table while no updates for that route are received. If the FortiGate unit receives an update for the route before the timeout period expires, the timer is restarted. The timeout period should be at least three times longer than the depute period, otherwise you will experience an error.

If you are experiencing problems with routers not responding in time to updates, increase this timer. However, remember that longer timeout intervals result in longer overall update periods — it may be considerable time before the time the FortiGate unit is done waiting for all the timers to expire on unresponsive routes.

Garbage timer

The garbage timer is the amount of time (in seconds) that the FortiGate unit will advertise a route as being unreachable before deleting the route from the routing table. If this timer is shorter, it will keep more up-to-date routes in the routing table and remove old ones faster. This will result in a smaller routing table which is useful if you have a very large network, or if your network changes frequently.

Authentication and key-chain

RIP version 2 uses authentication keys to ensure that the routing information exchanged between routers is reliable. RIP version 1 has no authentication. For authentication to work both the sending and receiving routers must be set to use authentication, and must be configured with the same keys.

The sending and receiving routers need to have their system dates and times synchronized to ensure both ends are using the same keys at the proper times. However, you can overlap the key lifetimes to ensure that a key is always available even if there is some difference in the system times.

A key chain is a list of one or more authentication keys including the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. The FortiGate unit migrates from one key to the next according to the scheduled send and receive lifetimes.

Key-chain is a CLI router command. You use this command to manage RIP version 2 authentication keys. You can add, edit or delete keys identified by the specified key number.

This example shows how to configure a key-chain with two keys that are valid sequentially in time. This example creates a key-chain called “rip_key” that has a password of “fortinet”. The accepted and send lifetimes are both set to the same values — a start time of 9:00am February 23, 2010 and an end time of 9:00am March 17, 2010. A second key is configured with a password of “my_fortigate” that is valid from March 17, 2010 9:01am to April 1 2010 9:00am. This “rip_key” keychain is then used on the port1 interface in RIP.

```
config router key-chain
```

```
    edit "rip_key"
       config key
       edit 1
          set accept-lifetime 09:00:00 23 02 2010 09:00:00 17 03 2010
          set key-string "fortinet"
          set send-lifetime 09:00:00 23 02 2010 09:00:00 17 03 2010
       next
       edit 2
          set accept-lifetime 09:01:00 17 03 2010 09:00:00 1 04 2010
          set key-string "my_fortigate"
          set send-lifetime 09:01:00 17 03 2010 09:00:00 1 04 2010
       next
       end
    end
config router rip
    config interface
       edit port1
          set auth-keychain "rip_key"
       end
    end
```

The CLI commands associated with authentication keys include:

```
config router key-chain

config router rip
    config interface
       edit <interface>
          set auth-keychain
          set auth-mode
          set auth-string
       end
    end
```

Access Lists

Access lists are filters used by FortiGate unit RIP and OSPF routing. An access list provides a list of IP addresses and the action to take for them — essentially an access list makes it easy to group addresses that will be treated the same into the same group, independent of their subnets or other matching qualities. You add a rule for each address or subnet that you want to include, specifying the action to take for it. For example if you wanted all traffic from one department to be routed a particular way, even in different buildings, you can add all the addresses to an access list and then handle that list all at once.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

Access lists greatly speed up configuration and network management. When there is a problem, you can check each list instead of individual addresses. Also its easier to troubleshoot since if all addresses on one list have problems, it eliminates many possible causes right away.

If you are using the RIPng or OSPF+ IPv6 protocols you will need to use access-list6, the IPv6 version of access list. The only difference is that access-list6 uses IPv6 addresses.

For example, if you want to create an access list called `test_list` that only allows an exact match of `10.10.10.10` and `11.11.11.11`, enter the command:

```
config router access-list
   edit test_list
      config rule
         edit 1
            set prefix 10.10.10.10 255.255.255.255
            set action allow
            set exact-match enable
         next
         edit 2
            set prefix 11.11.11.11 255.255.255.255
            set action allow
            set exact-match enable
         end
      end
```

Another example is if you want to deny ranges of addresses in IPv6 that start with the IPv6 equivalents of 10.10.10.10 and 11.11.11.11, enter the command access-list6 as follows:

```
config router access-list6
   edit test_list_ip6
      config rule
         edit 1
            set prefix6 2002:A0A:A0A:0:0:0:0:0:/48
            set action deny
         next
         edit 2
            set prefix6 2002:B0B:B0B:0:0:0:0:0/48
            set action deny
         end
      end
```

To use an access_list, you must call it from a routing protocol such as RIP. The following example uses the access_list from the earlier example called test_list to match routes coming in on the port1 interface. When there is a match, it will add 3 to the hop count metric for those routes to artificially increase . Enter the following command:

```
config router rip
   config offset-list
      edit 5
         set access-list test_list
         set direction in
         set interface port1
         set offset 3
         set status enable
      end
```

If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route, 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose

How RIP works

As one of the original modern dynamic routing protocols, RIP is straightforward. Its routing algorithm is not complex, there are some options to allow fine tuning, and it's relatively simple to configure RIP on FortiGate

units.

From RFC 1058:

> *Distance vector algorithms are based on the exchange of only a small amount of information. Each entity (gateway or host) that participates in the routing protocol is assumed to keep information about all of the destinations within the system. Generally, information about all entities connected to one network is summarized by a single entry, which describes the route to all destinations on that network.*

This section includes:

- RIP versus static routing
- RIP metric — hop count
- The Bellman–Ford routing algorithm
- Passive versus active RIP interfaces
- RIP packet structure

RIP versus static routing

RIP was one of the earliest dynamic routing protocols to work with IP addresses. As such, it is not as complex as more recent protocols. However, RIP is a big step forward from simple static routing.

While RIP may be slow in response to network outages, static routing has zero response. The same is true for convergence — static routing has zero convergence. Both RIP and static routing have the limited hop count, so its not a strength or a weakness. Count to infinity can be a problem, but typically can be fixed as it happens or is the result of a network outage that would cause even worse problems on static routing network.

This compares to static routing where each time a packet needs to be routed, the FortiGate unit can only send it to the next hop towards the destination. That next hop then forwards it, and so on until it arrives at its destination. RIP keeps more routing information on each router so your FortiGate unit can send the packet farther towards its destination before it has to be routed again towards its destination. RIP reduces the amount of table lookups and therefore fewer network resources than static routing. Also since RIP is updated on neighboring routes it is aware of new routes or dead routes that static routing would not be aware of.

Overall, RIP is a large step forward when compared to static routing.

RIP metric — hop count

RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the FortiGate unit, while a hop count of 16 represents a network that cannot be reached. Each network that a packet travels through to reach its destination usually counts as one hop. When the FortiGate unit compares two routes to the same destination, it adds the route having the lowest hop count to the routing table. As you can see in RIP packet structure on page 305, the hop count is part of a RIP v2 packet.

Similarly, when RIP is enabled on an interface, the FortiGate unit sends RIP responses to neighboring routers on a regular basis. The updates provide information about the routes in the FortiGate unit's routing table, subject to the rules that you specify for advertising those routes. You can specify how often the FortiGate unit sends updates, the period of time a route can be kept in the routing table without being updated, and for routes that are not updated regularly you can specify the period of time that the unit advertises a route as unreachable before it is removed from the routing table.

If hops are weighted higher than one, it becomes very easy to reach the upper limit. This higher weighting will effectively limit the size of your network depending on the numbers used. Merely changing from the default of 1.0 to 1.5 will lower the effective hop count from 15 to 10. This is acceptable for smaller networks, but can be a problem as your network expands over time.

In RIP, you can use the offset command to artificially increase the hop count of a route. Doing this will make this route less preferred, and in turn it will get less traffic. Offsetting routes is useful when you have network connections of different bandwidths, different levels of reliability, or different costs. In each of these situations you still want the redundancy of multiple route access, but you don't want the bulk of your traffic using these less preferred routes. For an example of RIP offset, see Access Lists on page 299.

The Bellman–Ford routing algorithm

The routing algorithm used by RIP was first used in 1967 as the initial routing algorithm of the ARPANET. The Bellman–Ford algorithm is distributed because it involves a number of nodes (routers) within an Autonomous system, and consists of the following steps:

1. Each node calculates the distances between itself and all other nodes within the AS and stores this information as a table.
2. Each node sends its table to all neighboring nodes.
3. When a node receives distance tables from its neighbors, it calculates the shortest routes to all other nodes and updates its own table to reflect any changes.

To examine how this algorithm functions let's look at a network with 4 routers — routers 1 through 4. The distance from router1 to router2 is 2 hops, 1 to 3 is 3 hops, and 2 to 3 is 4 hops. Router4 is only connected to routers 2 and 3, each distance being 2 hops.

1. Router1 finds all the distance to the other three routers — router 2 is 2, router 3 is 3. Router1 doesn't have a route to router 4.
2. Routers 2 through 4 do the same calculations from their point of views.
3. Once router 1 gets an update from router 2 or 3, it will get their route to router 4. At that point it now has a route to router 4 and installs that in its local table.
4. If router1 gets an update from router3 first, it has a hop count of 5 to reach router4. But when router2 sends its update, router1 will go with router2's shorter 4 hops to reach router4. Future updates don't change this unless they are shorter than 4 hops, or the routing table route goes down.

RIP algorithm example in 4 steps

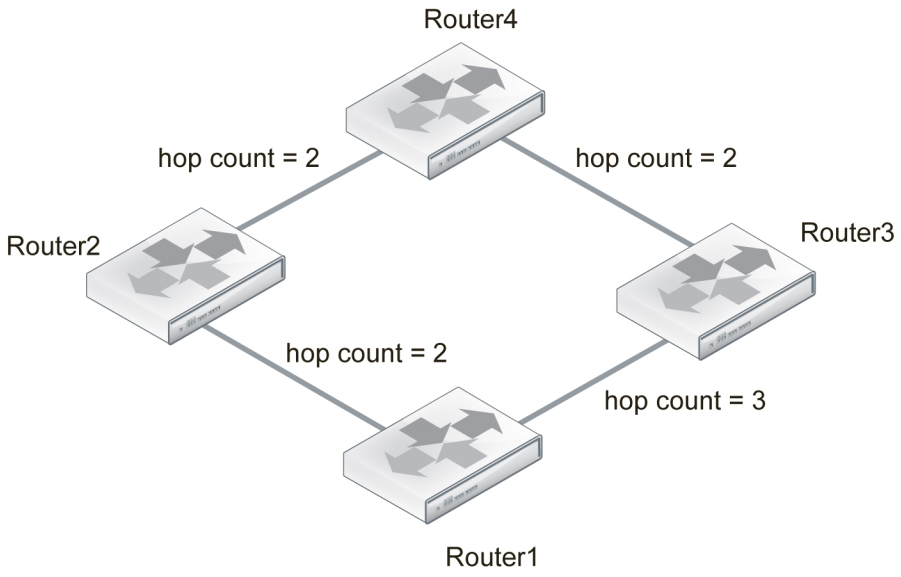
Step 1

Router1 finds the distance to other routers in the network.

It currently has no route to Router4.

Router1 routing table:

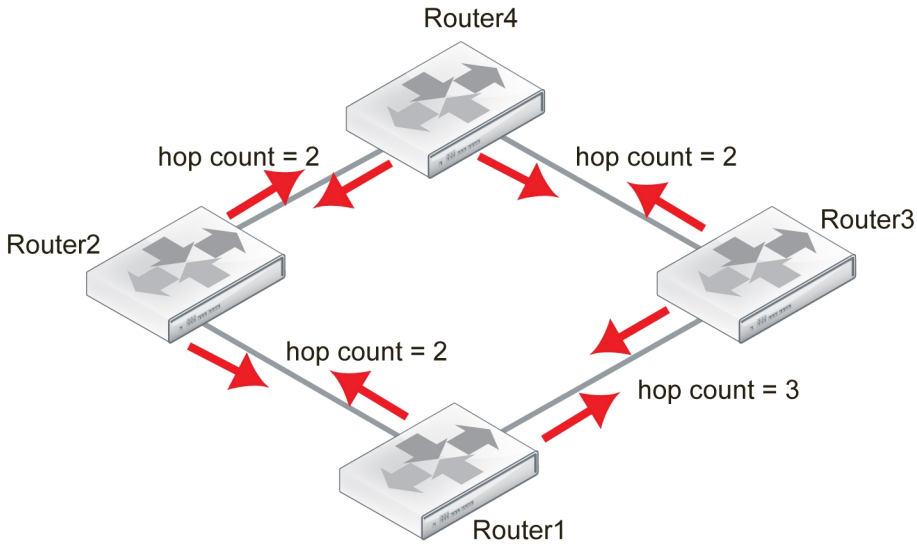
- Distance to Router2 = 2 hops.
- Distance to Router3 = 3 hops.



Step 2

All routers do the same as Router1, and send out updates containing their routing table.

Note that Router1 and Router4 do not update each other, but rely on Router2 and Router3 to pass along accurate updates.

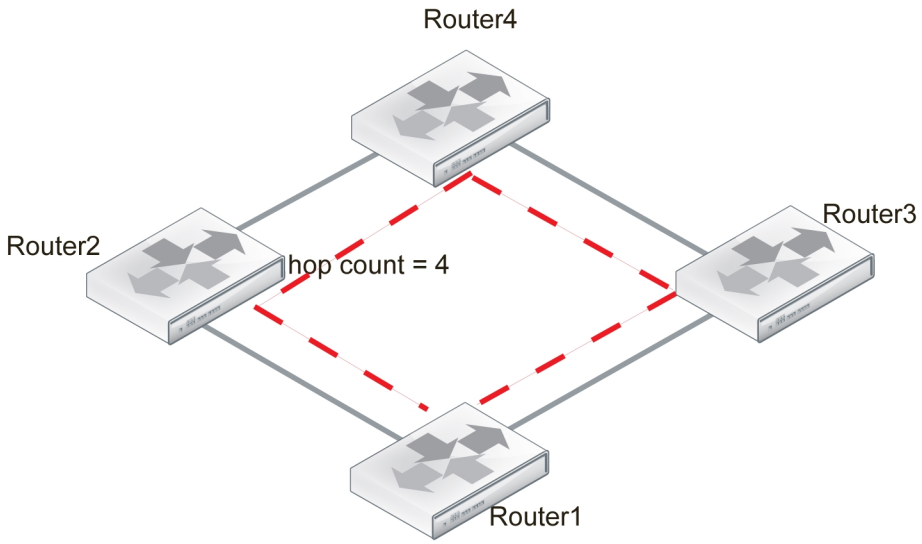


Step 3

Each router looks at the updates it has received, and adds any new or shorter routes to its table.

Router1 updated table:

- Distance to Router2 = 2 hops.
- Distance to Router3 = 3 hops.
- Distance to Router4 = 4 or 5 hops.

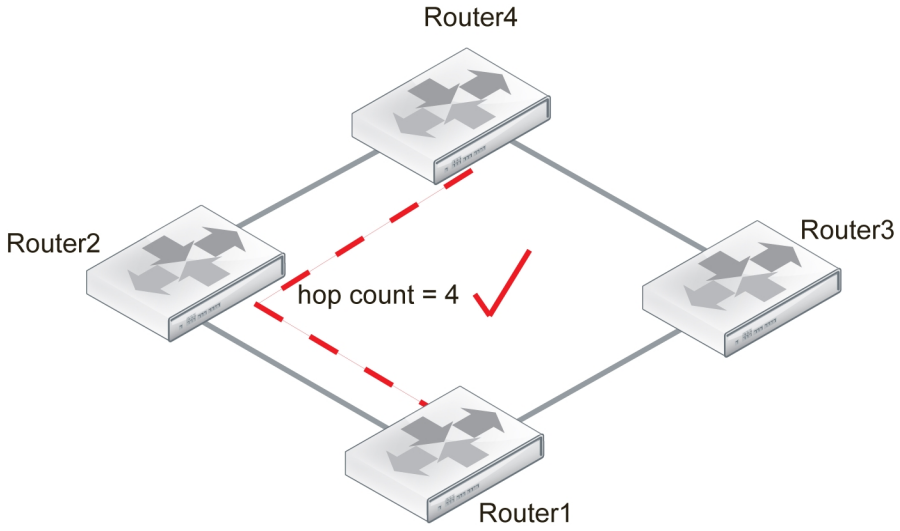


Step 4

Router1 installs the shortest route to Router4, and the other routes to it are removed from the routing table.

Router1 complete table:

- Distance to Router2 = 2 hops.
- Distance to Router3 = 3 hops.
- Distance to Router4 = 4 hops.



The good part about the Bellman-Ford algorithm in RIP is that the router only uses the information it needs from the update. If there are no newer, better routes than the ones the router already has in its routing table, there is no need to change its routing table. And no change means no additional update, so less traffic. But even when there is update traffic, the RIP packets are very small so it takes many updates to affect overall network bandwidth. For more information about RIP packets, see RIP packet structure on page 305.

The main disadvantage of the Bellman–Ford algorithm in RIP is that it doesn't take weightings into consideration. While it is possible to assign different weights to routes in RIP, doing so severely limits the effective network size

by reducing the hop count limit. Also other dynamic routing protocols can take route qualities, such as reliability or delay, into consideration to provide not only the physically shortest but also the fastest or more reliable routes as you choose.

Another disadvantage of the Bellman-Ford algorithm is due to the slow updates passed from one RIP router to the next. This results in a slow response to changes in the network topology, which in turn results in more attempts to use routes that are down, which wastes time and network resources.

Passive versus active RIP interfaces

Normally the FortiGate unit's routing table is kept up to date by periodically asking the neighbors for routes, and sending your routing updates out. This has the downside of generating a lot of extra traffic for large networks. The solution to this problem is passive interfaces.

An standard interface that supports RIP is active by default — it both sends and receives updates by actively communicating with its neighbors. A passive RIP interface does not send out updates — it just listens to the updates of other routers. This is useful in reducing network traffic, and if there are redundant routers in the network that would be sending out essentially the same updates all the time.

The following example shows how to create a passive RIP v2 interface on port1, using MD5 authentication and a key-chain called `passiveRIPv2` that has already been configured. Note that in the CLI, you enable passive by disabling `send-version2-broadcast`.

To create a passive RIP interface - web-based manager

1. Go to **Router > Dynamic > RIP**.
2. Next to **Interfaces**, select **Create**.
3. Select port1 as the **Interface**.
4. Select 2 as both the **Send Version** and **Receive Version**.
5. Select MD5 for **Authentication**.
6. Select the `passiveRIPv2` **Key-chain**.
7. Select **Passive Interface**.
8. Select **OK** to accept this configuration, and return to the main RIP display page.

To create a passive RIP v2 interface on port1 using MD5 authentication- CLI

```
config router rip
   config interface
      edit port1
         set send-version2-broadcast disable
         set auth-keychain "passiveRIPv2"
         set auth-mode md5
         set receive-version 2
         set send-version 2
      end
   end
```

RIP packet structure

It is hard to fully understand a routing protocol without knowing what information is carried in its packets. Knowing what information is exchanged between routers and how will help you better understand the RIP protocol, and better configure your network for it.

This section provides information on the contents of RIP 1 and RIP 2 packets.

RIP version 1

RIP version 1, or RIP IP packets are 24 bytes in length, with some empty areas left for future expansion.

RIP IP packets

1-byte command	1-byte version	2-byte zero field	2-byte AFI	2-byte zero field
4-byte IP address	4-byte zero field	4-byte zero field	4-byte metric	

A RIP 1 packet contains the following fields:

- **Command** — Indicates whether the packet is a request or a response. The request asks that a router send all or part of its routing table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing table entries. Multiple RIP packets are used to convey information from large routing tables.
- **Version** — Specifies the RIP version used. This field can signal different potentially incompatible versions.
- **Zero field** — This field defaults to zero, and is not used by RFC 1058 RIP.
- **Address-family identifier (AFI)** — Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address being specified. The AFI for IP is 2.
- **IP Address** — Specifies the IP address for the entry.
- **Metric** — This is the number of hops or routers traversed along the route on its trip to the destination. The metric is between 1 and 15 for that number of hops. If the route is unreachable the metric is 16.

RIP version 2

RIP version 2 has more features than RIP 1, which is reflected in its packets which carry more information. All but one of the empty zero fields in RIP 1 packets are used in RIP 2.

RIP 2 packets

1-byte command	1-byte version	2-byte unused	2-byte AFI	2-byte route tag
4-byte IP address	4-byte subnet	4-byte next hop	4-byte metric	

A RIP 2 packet contains fields described above in RIP 1, as well as the following:

- **Unused** — Has a value set to zero, and is intended for future use
- **Route tag** — Provides a method for distinguishing between internal routes learned by RIP and external routes learned from other protocols.
- **Subnet mask** — Contains the subnet mask for the entry. If this field is zero, no subnet mask has been specified for the entry.
- **Next hop** — Indicates the IP address of the next hop to which packets for the entry should be forwarded.

Troubleshooting RIP

This section is about troubleshooting RIP. For general troubleshooting information, see the FortiOS Handbook Troubleshooting chapter.

This section includes:

- Routing Loops
- Holddowns and Triggers for updates
- Split horizon and Poison reverse updates
- Debugging IPv6 on RIPng

Routing Loops

Normally in routing, a path between two addresses is chosen and traffic is routed along that path from one address to the other. When there is a routing loop, that normal path doubles back on itself creating a loop. When there are loops, the network has problems getting information to its destination and also prevents it from returning to the source to report the inaccessible destination.

A routing loop happens when a normally functioning network has an outage, and one or more routers are offline. When packets encounter this, an alternate route is attempted to maneuver around the outage. During this phase it is possible for a route to be attempted that involves going back a hop, and trying a different hop forward. If that hop forward is blocked by the outage as well, a hop back and possibly the original hop forward may be selected. You can see if this continues, how it can consume not only network bandwidth but also many resources on those routers affected. The worst part is this situation will continue until the network administrator changes the router settings, or the downed routers come back online.

Routing loops' effect on the network

In addition to this "traffic jam" of routed packets, every time the routing table for a router changes that router sends an update out to all of the RIP routers connected to it. In a network loop, its possible for a router to change its routes very quickly as it tries and fails along these new routes. This can quickly result in a flood of updates being sent out, which can effectively grind the network to a halt until the problem is fixed.

How can you spot a routing loop

Any time network traffic slows down, you will be asking yourself if it is a network loop or not. Often slowdowns are normal, they are not a full stoppage, and normal traffic resumes in a short period of time.

If the slow down is a full halt of traffic or a major slowdown does not return to normal quickly, you need to do serious troubleshooting quickly.

If you aren't running SNMP, dead gateway detection, or you have non-Fortinet routers in your network, you can use networking tools such as ping and traceroute to define the outage on your network and begin to fix it. Ping, traceroute, and other basic troubleshooting tools are largely the same between static and dynamic, and are covered in Advanced Static Routing on page 242.

Check your logs

If your routers log events to a central location, it can be easy to check the logs for your network for any outages.

On your FortiGate unit, go to **Log & Report**. You will want to look at both event logs and traffic logs. Events to look for will generally fall under CPU and memory usage, interfaces going offline (due to dead gateway detection), and other similar system events.

Once you have found and fixed your network problem, you can go back to the logs and create a report to better see how things developed during the problem. This type of forensics analysis can better help you prepare for next time.

Use SNMP network monitoring

If your network had no problems one minute and slows to a halt the next, chances are something changed to cause that problem. Most of the time an offline router is the cause, and once you find that router and bring it back online, things will return to normal.

If you can enable a hardware monitoring system such as SNMP or sFlow on your routers, you can be notified of the outage and where it is exactly as soon as it happens.

Ideally you can configure SNMP on all your FortiGate routers and be alerted to all outages as they occur.

To use SNMP to detect potential routing loops

1. Go to **System > Config > SNMP**.
2. Enable **SMTP Agent** and select **Apply**.
   Optionally enter the **Description**, **Location**, and **Contact** information for this device for easier location of the problem report.
3. Under **SNMP v1/v2** or **SNMP v3** as appropriate, select **Create New**.
   SNMP v3

User Name	Enter the SNMP user ID.
Security Level	Select authentication or privacy as desired. Select the authentication or privacy algorithms to use and enter the required passwords.
Notification Host	Enter the IP addresses of up to 16 hosts to notify.
Enable Query	Select. The **Port** should be 161. Ensure that your security policies allow ports 161 and 162 (SNMP queries and traps) to pass.

   SNMP v1/v2

Hosts	Enter the IP addresses of up to 8 hosts to notify. You can also specify the network **Interface**, or leave it as **ANY**.
Queries	Enable **v1** and/or **v2** as needed. The **Port** should be 161. Ensure that your security policies allow port 161 to pass.
Traps	Enable v1 and/or v2 as needed. The Port should be 162. Ensure that your security policies allow port 162 to pass.

4. Select the events for which you want notification. For routing loops this should include **CPU usage is high**, **Memory is low**, and possibly **Log disk space is low**.If there are problems the log will be filling up quickly, and the FortiGate unit's resources will be overused.

5. Configure SNMP host (manager) software on your administration computer. This will monitor the SNMP information sent out by the FortiGate unit. Typically you can configure this software to alert you to outages or CPU spikes that may indicate a routing loop.

Use Link Health Monitor and e-mail alerts

Another tool available to you on FortiGate units is the Link Health Monitor, useful in dead gateway detection. This feature allows the FortiGate unit to ping a gateway at regular intervals to ensure it is online and working. When the gateway is not accessible, that interface is marked as down.

To detect possible routing loops with Link Health Monitor and e-mail alerts

1. Go to **Router > Static > Settings** and select **Create New** under **Link Health Monitor**.
2. Enter the **Ping Server** IP address under **Gateway** and select the **Interface** that connects to it.
3. Set the **Probe Interval** (how often to send a ping), and **Failure Threshold** (how many lost pings is considered a failure). A smaller interval and smaller number of lost pings will result in faster detection, but will create more traffic on your network.

To configure notification of failed gateways

1. Go to **Log & Report > Report > Local** and enable **Email Generated Reports**.
2. Enter your email details.
3. Select **Apply**.

You might also want to log CPU and Memory usage as a network outage will cause your CPU activity to spike.

If you have VDOMs configured, you will have to enter the basic SMTP server information in the Global section, and the rest of the configuration within the VDOM that includes this interface.

After this configuration, when this interface on the FortiGate unit cannot connect to the next router, the FortiGate unit will bring down the interface and alert you with an email about the outage.

Look at the packet flow

If you want to see what is happening on your network, look at the packets travelling on the network. This is same idea as police pulling over a car and asking the driver where they have been, and what the conditions were like.

The method used in the troubleshooting sections Debugging IPv6 on RIPng on page 310 and on debugging the packet flow apply here as well. In this situation, you are looking for routes that have metrics higher than 15 as that indicates they are unreachable.

Ideally if you debug the flow of the packets, and record the routes that are unreachable, you can create an accurate picture of the network outage.

Action to take on discovering a routing loop

Once you have mapped the problem on your network, and determined it is in fact a routing loop there are a number of steps to take in correcting it.

1. Get any offline routers back online. This may be a simple reboot, or you may have to replace hardware. Often this first step will restore your network to its normal operation, once the routing tables finish being updated.

2. Change your routing configuration on the edges of the outage. Even if step 1 brought your network back online, you should consider making changes to improve your network before the next outage occurs. These changes can include configuring features like holddowns and triggers for updates, split horizon, and poison reverse updates.

Holddowns and Triggers for updates

One of the potential problems with RIP is the frequent routing table updates that are sent every time there is a change to the routing table. If your network has many RIP routers, these updates can start to slow down your network. Also if you have a particular route that has bad hardware, it might be going up and down frequently, which will generate an overload of routing table updates.

One of the most common solutions to this problem is to use holddown timers and triggers for updates. These slow down the updates that are sent out, and help prevent a potential flood.

Holddown Timers

The holddown timer activates when a route is marked down. Until the timer expires, the router does not accept any new information about that route. This is very useful if you have a flapping route because it will prevent your router from sending out updates and being part of the problem in flooding the network. The potential down side is if the route comes back up while the timer has not expired, that route will be unavailable for that period of time. This is only a problem if this is a major route used by the majority of your traffic. Otherwise, this is a minor problem as traffic can be re-routed around the outage.

Triggers

Triggered RIP is an alternate update structure that is based around limiting updates to only specific circumstances. The most basic difference is that the routing table will only be updated when a specific request is sent to update, as opposed to every time the routing table changes. Updates are also triggered when a unit is ‘powered on’, which can include addition of new interfaces or devices to the routing structure, or devices returning to being available after being unreachable.

Split horizon and Poison reverse updates

Split horizon is best explained with an example. You have three routers linked serially, let’s call them A, B, and C. A is only linked to B, C is only linked to B, and B is linked to both A and C. To get to C, A must go through B. If the link to C goes down, it is possible that B will try to use A’s route to get to C. This route is A-B-C, so it will loop endlessly between A and B.

This situation is called a split horizon because from B’s point of view the horizon stretches out in each direction, but in reality it only is on one side.

Poison reverse is the method used to prevent routes from running into split horizon problems. Poison reverse “poisons” routes away from the destination that use the current router in their route to the destination. This “poisoned” route is marked as unreachable for routers that cannot use it. In RIP this means that route is marked with a distance of 16.

Debugging IPv6 on RIPng

The debug commands are very useful to see what is happening on the network at the packet level. There are a few changes to debugging the packet flow when debugging IPv6.

The following CLI commands specify both IPv6 and RIP, so only RIPng packets will be reported. The output from these commands will show you the RIPng traffic on your FortiGate unit including RECV, SEND, and UPDATE actions.

The addresses are in IPv6 format.

```
diagnose debug enable
diagnose ipv6 router rip level info
diagnose ipv6 router rip all enable
```

These three commands will:

- turn on debugging in general
- set the debug level to information, a verbose reporting level
- turn on all rip router settings

Part of the information displayed from the debugging is the metric (hop count). If the metric is 16, then that destination is unreachable since the maximum hop count is 15.

In general, you should see an update announcement, followed by the routing table being sent out, and a received reply in response.

For more information, see Troubleshooting RIP on page 307.

Simple RIP example

This is an example of a typical medium sized network configuration using RIP routing.

Your company has 3 small local networks, one for each department. These networks are connected by RIP, and then connected to the Internet. Each subnet has more than one route, for redundancy. There are two central routers that are both connected to the Internet, and to the other networks. If one of those routers goes down, the whole network can continue to function normally.

The ISP is running RIP, so no importing or exporting routes is required on the side of the network. However, since the internal networks have static networking running those will need to be redistributed through the RIP network.

To keep the example simple, there will be no authentication of router traffic.

With RIP properly configured, if the device fails or temporarily goes offline, the routes will change and traffic will continue to flow. RIP is good for a smaller network due to its lack of complex configurations.

This section includes the following topics:

- Network layout and assumptions
- General configuration steps
- Configuring the FortiGate units system information
- Configuring other networking devices
- Testing network configuration

Network layout and assumptions

Basic network layout

Your company has 3 departments each with their own network — Sales, R&D, and Accounting. Each network has routers that are not running RIP as well as FortiGate units running RIP.

The R&D network has two RIP routers, and each is connected to both other departments as well as being connected to the Internet through the ISP router. The links to the Internet are indicated in black.

The three internal networks do not run RIP. They use static routing because they are small networks. This means the FortiGate units have to redistribute any static routes they learn so that the internal networks can communicate with each other.

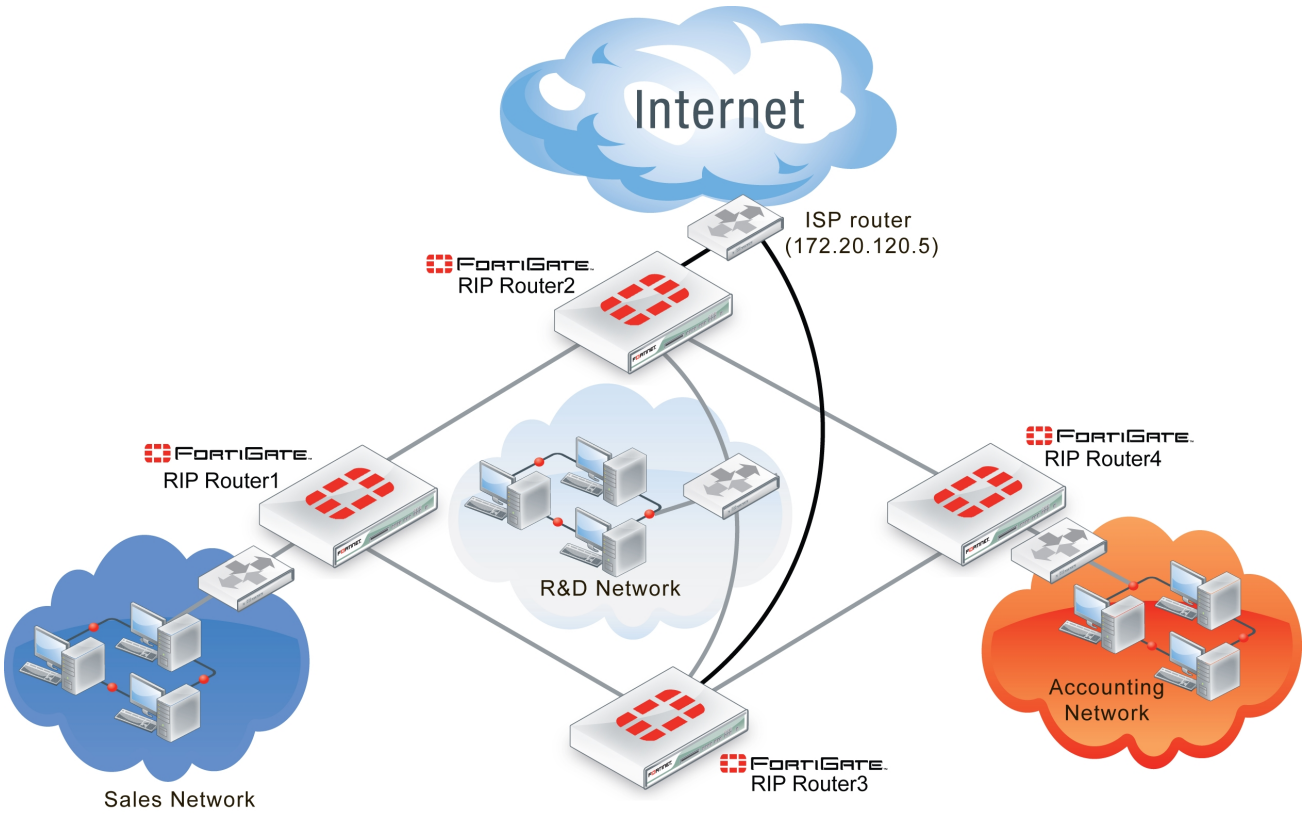
Where possible in this example, the default values will be used or the most general settings. This is intended to provide an easier configuration that will require less troubleshooting.

In this example the routers, networks, interfaces used, and IP addresses are as follows. Note that the Interfaces that connect Router2 and Router3 also connect to the R&D network.

RIP example network topology

Network	Router	Interface & Alias	IP address
Sales	Router1	port1 (internal)	10.11.101.101
		port2 (router2)	10.11.201.101
		port3 (router3)	10.11.202.101
	Router2	port1 (internal)	10.12.101.102
		port2 (router1)	10.11.201.102
		port3 (router4)	10.14.201.102
		port4 (ISP)	172.20.120.102
R&D	Router3	port1 (internal)	10.12.101.103
		port2 (router1)	10.11.201.103
		port3 (router4)	10.14.202.103
		port4 (ISP)	172.20.120.103
	Router4	port1 (internal)	10.14.101.104
Accounting		port2 (router2)	10.14.201.104
		port3 (router3)	10.14.202.104

Network topology for the simple RIP example



Assumptions

The following assumptions have been made concerning this example.

- All FortiGate units have 5.0 firmware, and are running factory default settings.
- All CLI and web-based manager navigation assumes the unit is running in NAT/Route operating mode, with VDOMs disabled.
- All FortiGate units have interfaces labelled port1 through port4 as required.
- All firewalls have been configured for each FortiGate unit to allow the required traffic to flow across interfaces.
- Only FortiGate units are running RIP on the internal networks.
- Router2 and Router3 are connected through the internal network for R&D.
- Router2 and Router3 each have their own connection to the Internet, indicated in black in the diagram above.

General configuration steps

This example is very straight forward. The only steps involved are:

- Configuring the FortiGate units system information
- Configuring FortiGate unit RIP router information
- Configuring other networking devices
- Testing network configuration

Configuring the FortiGate units system information

Each FortiGate unit needs their hostname, and interfaces configured.

For IP numbering, Router2 and Router3 use the other routers numbering where needed.

Router2 and Router3 have dead gateway detection enabled on the ISP interfaces using Ping. Remember to contact the ISP and confirm their server has ping enabled.

Configure the hostname, interfaces, and default route

To configure Router1 system information - web-based manager

1. Go to **System > Dashboard > Status > System Information**.
2. Next to **Host Name** select **Change**, and enter “Router1”.
3. Go to **Router > Static > Static Routes**.
4. Edit the default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2 (router2)
Gateway	172.20.120.5/255.255.255.0
Distance	40

5. Enter a second default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3 (router3)
Gateway	172.20.120.5/255.255.255.0
Distance	40

6. Go to **System > Network > Interfaces**.
7. Edit port1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.101/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Internal sales network
Administrative Status	Up

9. Edit port2 (router2) interface.
10. Set the following information, and select **OK**.

Alias	router2
IP/Network Mask	10.11.201.101/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to R&D network & Internet through Router2
Administrative Status	Up

11. Edit port3 (router3) interface.
12. Set the following information, and select **OK**.

Alias	router3
IP/Network Mask	10.11.202.101/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to R&D network and Internet through Router3
Administrative Status	Up

To configure Router1 system information - CLI

```
config system global
   set hostname Router1
end

config router static
   edit 1
      set device "port2"
      set distance 45
      set gateway 10.11.201.102
   next
   edit 2
      set device “port3”
      set distance 45
      set gateway 10.11.202.103
   end
end


config system interface
   edit port1
      set alias internal
      set ip 10.11.101.101/255.255.255.0
      set allowaccess https ssh ping
      set description “Internal sales network”
   next
   edit port2
      set alias ISP
      set allowaccess https ssh ping
      set ip 10.11.201.101/255.255.255.0
      set description “Link to R&D network & Internet through Router2”
   next
```

```
    edit port3
       set alias router3
       set ip 10.11.202.101/255.255.255.0
       set allowaccess https ssh ping
       set description "Link to R&D network & Internet through Router2"
    end
end
```

To configure Router2 system information - web-based manager

1. Go to **System > Dashboard > Status > System Information**.
2. Next to **Host Name** select **Change**, and enter "Router2".
3. Go to **Router > Static > Static Routes**.
4. Edit the default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port4 (ISP)
Gateway	172.20.120.5/255.255.255.0
Distance	5

5. Go to **System > Network > Interfaces**.
6. Edit port1 (internal) interface.
7. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.12.101.102/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	R&D internal network and Router3
Administrative Status	Up

8. Edit port2 (router1) interface.
9. Set the following information, and select **OK**.

Alias	router1
IP/Network Mask	10.12.201.102/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to Router1 and the Sales network
Administrative Status	Up

10. Edit port3 (router4) interface.
11. Set the following information, and select **OK**.

Alias	router4
IP/Network Mask	10.12.301.102/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to Router4 and the accounting network
Administrative Status	Up

12. Edit port4 (ISP) interface.
13. Set the following information, and select **OK**.

Alias	ISP
IP/Network Mask	172.20.120.102/255.255.255.0
Administrative Access	HTTPS SSH PING
Detect and Identify Devices	enable
Description	Internet through ISP
Administrative Status	Up

To configure Router2 system information - CLI

```
config system global
   set hostname Router2
end
config router static
   edit 1
      set device "port4"
      set distance 5
      set gateway 172.20.130.5
   end
end
config system interface
   edit port1
      set alias internal
      set ip 10.11.101.102/255.255.255.0
      set allowaccess https ssh ping
      set description “Internal RnD network and Router3”
   next
   edit port2
      set alias router1
      set allowaccess https ssh ping
      set ip 10.11.201.102/255.255.255.0
      set description “Link to Router1”
   next
   edit port3
      set alias router3
      set ip 10.14.202.102/255.255.255.0
      set allowaccess https ssh ping
      set description “Link to Router4”
   next
```

```
    edit port4
       set alias ISP
       set ip 172.20.120.102/255.255.255.0
       set allowaccess https ssh ping
       set description "ISP and Internet"
    end
end
```

To configure Router3 system information - web-based manager

1. Go to **System > Dashboard > Status > System Information**.
2. Next to **Host Name** select **Change**, and enter "Router3".
3. Go to **Router > Static > Static Routes**.
4. Edit the default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port4 (ISP)
Gateway	172.20.120.5/255.255.255.0
Distance	5

5. Go to **System > Network > Interfaces**.
6. Edit port1 (internal) interface.
7. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.12.101.103/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	R&D internal network and Router2
Administrative Status	Up

8. Edit port2 (router1) interface.
9. Set the following information, and select **OK**.

Alias	router1
IP/Network Mask	10.13.201.103/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to Router1 and Sales network
Administrative Status	Up

10. Edit port3 (router4) interface.
11. Set the following information, and select **OK**.

Alias	router4
IP/Network Mask	10.13.301.103/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to Router4 and accounting network
Administrative Status	Up

12. Edit port4 (ISP) interface.
13. Set the following information, and select **OK**.

Alias	ISP
IP/Network Mask	172.20.120.103/255.255.255.0
Administrative Access	HTTPS SSH PING
Detect and Identify Devices	enable
Description	Internet and ISP
Administrative Status	Up

To configure Router3 system information - CLI

```
config system global
   set hostname Router3
end
config router static
   edit 1
      set device "port4"
      set distance 5
      set gateway 172.20.130.5
   end
end
config system interface
   edit port1
      set alias internal
      set ip 10.12.101.103/255.255.255.0
      set allowaccess https ssh ping
      set description “Internal RnD network and Router2”
   next
   edit port2
      set alias ISP
      set allowaccess https ssh ping
      set ip 10.11.201.103/255.255.255.0
      set description “Link to Router1”
   next
   edit port3
      set alias router3
      set ip 10.14.202.103/255.255.255.0
      set allowaccess https ssh ping
      set description “Link to Router4”
   next
```

```
    edit port4
       set alias ISP
       set ip 172.20.120.103/255.255.255.0
       set allowaccess https ssh ping
       set description "ISP and Internet"
    end
end
```

To configure Router4 system information - web-based manager

1. Go to **System > Dashboard > Status > System Information**.
2. Next to **Host Name** select **Change**, and enter "Router4".
3. Go to **Router > Static > Static Routes**.
4. Edit the default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2 (router2)
Gateway	172.20.120.5/255.255.255.0
Distance	40

5. Enter a second default route and enter the following information:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3 (router3)
Gateway	172.20.120.5/255.255.255.0
Distance	40

6. Go to **System > Network > Interfaces**.
7. Edit port 1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.14.101.104/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Internal accounting network
Administrative Status	Up

9. Edit port 2 (router2) interface.
10. Set the following information, and select **OK**.

Alias	router2

IP/Network Mask	10.14.201.104/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to R&D network & Internet through Router2
Administrative Status	Up

11. Edit port 3 (router3) interface.
12. Set the following information, and select **OK**.

Alias	router3
IP/Network Mask	10.14.301.104/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Link to R&D network and Internet through Router3
Administrative Status	Up

To configure Router4 system information - CLI

```
config system global
   set hostname Router4
end
config router static
   edit 1
      set device "port2"
      set distance 45
      set gateway 10.14.201.102
   next
   edit 2
      set device “port3”
      set distance 45
      set gateway 10.14.202.103
   end
end
config system interface
   edit port1
      set alias internal
      set ip 10.14.101.104/255.255.255.0
      set allowaccess https ssh ping
      set description “Internal sales network”
   next
   edit port2
      set alias router2
      set allowaccess https ssh ping
      set ip 10.14.201.104/255.255.255.0
      set description “Link to R&D network & Internet through Router2”
   next
   edit port3
      set alias router3
      set ip 10.14.202.104/255.255.255.0
      set allowaccess https ssh ping
```

```
        set description "Link to R&D network & Internet through Router2"
    end
end
```

Configuring FortiGate unit RIP router information

With the interfaces configured, RIP can now be configured on the FortiGate units.

For each FortiGate unit the following steps will be taken:

- Configure RIP version used
- Redistribute static networks
- Add networks serviced by RIP
- Add interfaces that support RIP on the FortiGate unit

Router1 and Router4 are configured the same. Router2 and Router3 are configured the same. These routers will be grouped accordingly for the following procedures — repeat the procedures once for each FortiGate unit.

Configure RIP settings on Router1 and Router4 - web-based manager

1. Go to **Router > Dynamic > RIP**.
2. Select **2** for **RIP Version**.
3. In **Advanced Options**, under **Redistribute** enable **Static**.
4. Leave the other Advanced Options at default values.
5. Enter the following networks, and select **Add** after each:
   - 10.11.0.0/255.255.0.0
   - 10.12.0.0/255.255.0.0
   - 10.14.0.0/255.255.0.0
   - 172.20.120.0/255.255.255.0
6. For interface, select **Create** and set the following information.

Interface	port1 (internal)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

7. For interface, select **Create** and set the following information.

Interface	port2 (router2)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

8. For interface, select **Create** and set the following information.

Interface	port3 (router3)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

Configure RIP settings on Router1 and Router4 - CLI

```
config router rip
   set version 2
   config interface
      edit "port1"
         set receive-version 1 2
         set send-version 1 2
      next
      edit "port2"
         set receive-version 1 2
         set send-version 1 2
      next
      edit "port3"
         set receive-version 1 2
         set send-version 1 2
      end
   config network
      edit 1
         set prefix 10.11.0.0 255.255.0.0
      next
      edit 2
         set prefix 10.12.0.0 255.255.0.0
      next
      edit 3
         set prefix 10.14.0.0 255.255.0.0
      next
      edit 4
         set prefix 172.20.120.0 255.255.255.0
      end
   config redistribute "static"
      set status enable
   end
end
```

Configure RIP settings on Router2 and Router3- web-based manager

1. Go to **Router > Dynamic > RIP**.
2. Select **2** for **RIP Version**.
3. In **Advanced Options**, under **Redistribute** enable **Static**.
4. Leave the other Advanced Options at default values.
5. Enter the following networks, and select **Add** after each:

- 10.11.0.0/255.255.0.0
- 10.12.0.0/255.255.0.0
- 10.14.0.0/255.255.0.0
- 172.20.120.0/255.255.255.0

6. For interface, select **Create** and set the following information.

Interface	port1 (internal)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

7. For interface, select **Create** and set the following information.

Interface	port2 (router1)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

8. For interface, select **Create** and set the following information.

Interface	port3 (router4)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

9. For interface, select **Create** and set the following information.

Interface	port4 (ISP)
Send Version	Both
Receive Version	Both
Authentication	None
Passive Interface	disabled

Configure RIP settings on Router2 and Router3- web-based manager

```
config router rip
   set version 2
   config interface
      edit "port1"
         set receive-version 1 2
         set send-version 1 2
      next
      edit "port2"
         set receive-version 1 2
         set send-version 1 2
      next
      edit "port3"
         set receive-version 1 2
         set send-version 1 2
      end
      edit "port4"
         set receive-version 1 2
         set send-version 1 2
      end
   config network
      edit 1
         set prefix 10.11.0.0 255.255.0.0
      next
      edit 2
         set prefix 10.12.0.0 255.255.0.0
      next
      edit 3
         set prefix 10.14.0.0 255.255.0.0
      next
      edit 4
         set prefix 172.20.120.0 255.255.255.0
      end
   config redistribute "static"
      set status enable
   end
end
```

Configuring other networking devices

In this example there are two groups of other devices on the the network — internal devices, and the ISP.

The first is the internal network devices on the Sales, R&D, and Accounting networks. This includes simple static routers, computers, printers and other network devices. Once the FortiGate units are configured, the internal static routers need to be configured using the internal network IP addresses. Otherwise there should be no configuration required.

The second group of devices is the ISP. This consists of the RIP router the FortiGate routers 2 and 3 connect to. You need to contact your ISP and ensure they have your information for your network such as the IP addresses of the connecting RIP routers, what version of RIP your network supports, and what authentication (if any) is used.

Testing network configuration

Once the network has been configured, you need to test that it works as expected.

The two series of tests you need to run are to test the internal networks can communicate with each other, and that the internal networks can reach the Internet.

Use ping, traceroute, and other networking tools to run these tests.

If you encounter problems, for troubleshooting help consult Simple RIP example on page 311.

RIPng — RIP and IPv6

RIP next generation, or RIPng, is the version of RIP that supports IPv6.

This is an example of a typical small network configuration using RIPng routing.

Your internal R&D network is working on a project for a large international telecom company that uses IPv6. For this reason, you have to run IPv6 on your internal network and you have decided to use only IPv6 addresses.

Your network has two FortiGate units running the RIPng dynamic routing protocol. Both FortiGate units are connected to the ISP router and the internal network. This configuration provides some redundancy for the R&D internal network enabling it to reach the Internet at all times.

This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate units system information
- Configuring RIPng on FortiGate units
- Configuring other network devices
- Testing the configuration

Network layout and assumptions

Basic network layout

Your internal R&D network is working on a project for a large international telecom company that uses IPv6. For this reason, you have to run IPv6 on your internal network and you have decided to use only IPv6 addresses.

Your network has two FortiGate units running the RIPng dynamic routing protocol. Both FortiGate units are connected to the ISP router and the internal network. This configuration provides some redundancy for the R&D internal network enabling it to reach the Internet at all times.

All internal computers use RIP routing, so no static routing is required. And all internal computers use IPv6 addresses.

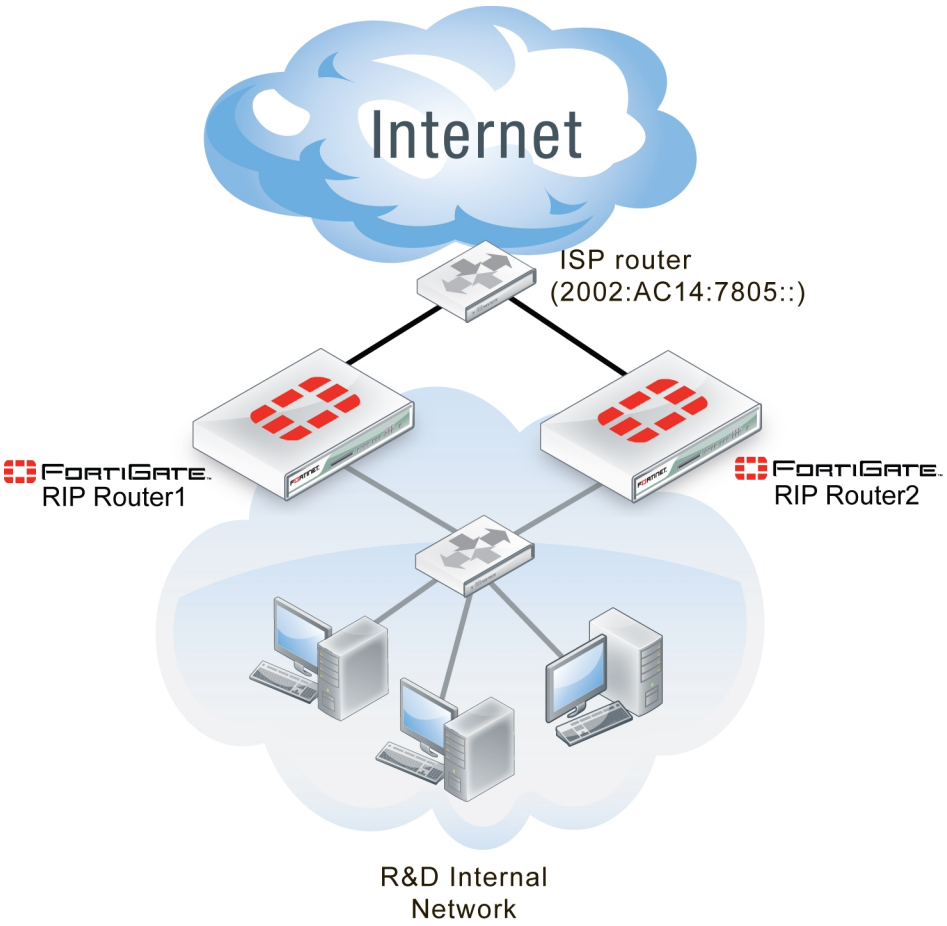
Where possible in this example, the default values will be used or the most general settings. This is intended to provide an easier configuration that will require less troubleshooting.

In this example the routers, networks, interfaces used, and IP addresses are as follows.

RIP example network topology

Network	Router	Interface & Alias	IPv6 address
R&D	Router1	port1 (internal)	2002:A0B:6565:0:0:0:0:0
		port2 (ISP)	2002:AC14:7865:0:0:0:0:0
	Router2	port1 (internal)	2002:A0B:6566:0:0:0:0:0
		port2 (ISP)	2002:AC14:7866:0:0:0:0:0

Network topology for the IPV6 RIPng example



Assumptions

The following assumptions have been made concerning this example.

- All FortiGate units have 5.0 firmware, and are running factory default settings.
- All CLI and web-based manager navigation assumes the unit is running in NAT/Route operating mode, with VDOMs disabled.
- All FortiGate units have interfaces labelled port1 and port2 as required.

- All firewalls have been configured for each FortiGate unit to allow the required traffic to flow across interfaces.
- All network devices are support IPv6 and are running RIPng.

Configuring the FortiGate units system information

Each FortiGate unit needs IPv6 enabled, a new hostname, and interfaces configured.

To configure system information on Router1 - web-based manager

1. Go to **System > Dashboard > Status**.
2. For **Host name**, select **Change**.
3. Enter “Router1”.
4. Go to **System > Config > Features**.
5. In **Basic Features**, enable **IPv6**, and select **Apply**.
6. Go to **System > Network > Interfaces**.
7. Edit port1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	2002:A0B:6565::/0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

9. Edit port2 (ISP) interface.
10. Set the following information, and select **OK**.

Alias	ISP
IP/Network Mask	2002:AC14:7865::/0
Administrative Access	HTTPS SSH PING
Description	ISP and Internet
Administrative Status	Up

To configure system information on Router1 - CLI

```
config system global
   set hostname Router1
   set gui-ipv6 enable
end
config system interface
   edit port1
      set alias internal
      set allowaccess https ping ssh
      set description “Internal RnD network”
      config ipv6
```

```
      set ip6-address 2002:a0b:6565::/0
   end
next
edit port2
   set alias ISP
   set allowaccess https ping ssh
   set description "ISP and Internet"
   config ipv6
      set ip6-address 2002:AC14:7865::
   end
end
```

To configure system information on Router2 - web-based manager

1. Go to **System > Dashboard > Status**.
2. For **Host name**, select **Change**.
3. Enter "Router2".
4. Go to **System > Config > Features**.
5. In **Basic Features**, enable **IPv6**, and select **Apply**.
6. Go to **System > Network > Interfaces**.
7. Edit port1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	2002:A0B:6566::/0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

9. Edit port2 (ISP) interface.
10. Set the following information, and select **OK**.

Alias	ISP
IP/Network Mask	2002:AC14:7866::/0
Administrative Access	HTTPS SSH PING
Description	ISP and Internet
Administrative Status	Up

To configure system information on Router2 - CLI

```
config system global
   set hostname Router2
   set gui-ipv6 enable
end
config system interface
```

```
edit port1
   set alias internal
   set allowaccess https ping ssh
   set description "Internal RnD network"
   config ipv6
      set ip6-address 2002:a0b:6566::/0
   end
next
edit port2
   set alias ISP
   set allowaccess https ping ssh
   set description "ISP and Internet"
   config ipv6
      set ip6-address 2002:AC14:7866::
   end
end
```

Configuring RIPng on FortiGate units

Now that the interfaces are configured, you can configure RIPng on the FortiGate units.

There are only two networks and two interfaces to include — the internal network, and the ISP network. There is no redistribution, and no authentication. In RIPng there is no specific command to include a subnet in the RIP broadcasts. There is also no information required for the interfaces beyond including their name.

As this is a CLI only configuration, configure the ISP router and the other FortiGate unit as neighbors. This was not part of the previous example as this feature is not offered in the web-based manager. Declaring neighbors in the configuration like this will reduce the discovery traffic when the routers start up.

Since RIPng is not supported in the web-based manager, this section will only be entered in the CLI.

To configure RIPng on Router1 - CLI

```
config router ripng
   config interface
      edit port1
      next
      edit port2
      end
   config neighbor
      edit 1
         set interface port1
         set ipv6 2002:a0b:6566::/0
      next
      edit 2
         set interface port2
         set ipv6 2002:AC14:7805::/0
      end
```

To configure RIPng on Router2 - CLI

```
config router ripng
   config interface
      edit port1
      next
      edit port2
      end
```

```
config neighbor
   edit 1
      set interface port1
      set ipv6 2002:a0b:6565::/0
   next
   edit 2
      set interface port2
      set ipv6 2002:AC14:7805::/0
   end
```

Configuring other network devices

The other devices on the internal network all support IPv6, and are running RIPng where applicable. They only need to know the internal interface network addresses of the FortiGate units.

The ISP routers need to know the FortiGate unit information such as IPv6 addresses.

Testing the configuration

In addition to normal testing of your network configuration, you must also test the IPv6 part of this example.

For troubleshooting problems with your network, see the FortiOS Handbook Troubleshooting chapter.

For troubleshooting problems with RIP, see RIPng — RIP and IPv6 on page 326.

Testing the IPv6 RIPng information

There are some commands to use when checking that your RIPng information is correct on your network. These are useful to check on your RIPng FortiGate units on your network. Comparing the output between devices will help you understand your network better, and also track down any problems.

```
diagnose ipv6 address list
```

View the local scope IPv6 addresses used as next-hops by RIPng on the FortiGate unit.

```
diagnose ipv6 route list
```

View ipv6 addresses that are installed in the routing table.

```
get router info6 routing-table
```

View the routing table. This information is almost the same as the previous command (diagnose ipv6 route list) however it is presented in an easier to read format.

```
get router info6 rip interface external
```

View brief output on the RIP information for the interface listed. The information includes if the interface is up or down, what routing protocol is being used, and whether passive interface or split horizon are enabled.

```
get router info6 neighbor-cache list
```

View the IPv6/MAC address mapping. This also displays the interface index and name associated with the address.

Border Gateway Protocol (BGP)

This section describes Border Gateway Protocol (BGP).

The following topics are included in this section:

BGP background and concepts
Troubleshooting BGP
Dual-homed BGP example
Redistributing and blocking routes in BGP

BGP background and concepts

The border gateway protocol contains two distinct subsets — internal BGP (iBGP) and external BGP (eBGP). iBGP is intended for use within your own networks. eBGP is used to connect many different networks together, and is the main routing protocol for the Internet backbone. FortiGate units support iBGP, and eBGP only for communities.

The following topics are included in this section:

- Background
- Parts and terminology of BGP
- How BGP works

Background

BGP was first used in 1989. The current version, BGP-4, was released in 1995 and is defined in RFC 1771. That RFC has since been replaced by the more recent RFC 4271. The main benefits of BGP-4 are classless inter-domain routing, and aggregate routes. BGP is the only routing protocol to use TCP for a transport protocol. Other routing protocols use UDP.

BGP makes routing decisions based on path, network policies and rulesets instead of the hop-count metric as RIP does, or cost-factor metrics as OSPF does.

BGP-4+ supports IPv6. It was introduced in RFC 2858 and RFC 2545.

BGP is the routing protocol used on the Internet. It was designed to replace the old Exterior Gateway Protocol (EGP) which had been around since 1982, and was very limited. In doing so, BGP enabled more networks to take part in the Internet backbone to effectively decentralize it and make the Internet more robust, and less dependent on a single ISP or backbone network.

Parts and terminology of BGP

In a BGP network, there are some terms that need to be explained before going ahead. Some parts of BGP are not explained here as they are common to other dynamic routing protocols as well. When determining your network topology, note that the number of available or supported routes is not set by the configuration but depends on your FortiGate's available memory. For more information on parts of BGP that are not listed here, see Dynamic Routing Overview on page 279.

BGP and IPv6

FortiGate units support IPv6 over BGP using the same `config router bgp` command as IPv4, but different subcommands.

The main CLI keywords have IPv6 equivalents that are identified by the “6” on the end of the keyword, such as with `config network6` or `set allowas-in6`. For more information about IPv6 BGP keywords, see the FortiGate CLI Reference.

IPv6 BGP commands include:

```
config router bgp
   set activate6 {enable | disable}
   set allowas-in6 <max_num_AS_integer>
   set allowas-in-enable6 {enable | disable}
   set as-override6 {enable | disable}
   set attribute-unchanged6 [as-path] [med] [next-hop]
   set capability-default-originate6 {enable | disable}
   set capability-graceful-restart6 {enable | disable}
   set capability-orf6 {both | none | receive | send}
   set default-originate-route-map6 <routemap_str>
   set distribute-list-in6 <access-list-name_str>
   set distribute-list-out6 <access-list-name_str>
   set filter-list-in6 <aspath-list-name_str>
   set filter-list-out6 <aspath-list-name_str>
   set maximum-prefix6 <prefix_integer>
   set maximum-prefix-threshold6 <percentage_integer>
   set maximum-prefix-warning-only6 {enable | disable}
   set next-hop-self6 {enable | disable}
   set prefix-list-in6 <prefix-list-name_str>
   set prefix-list-out6 <prefix-list-name_str>
   set remove-private-as6 {enable | disable}
   set route-map-in6 <routemap-name_str>
   set route-map-out6 <routemap-name_str>
   set route-reflector-client6 {enable | disable}
   set route-server-client6 {enable | disable}
   set send-community6 {both | disable | extended | standard}
   set soft-reconfiguration6 {enable | disable}
   set unsuppress-map6 <route-map-name_str>
   config network6
   config redistribute6
end
```

Roles of routers in BGP networks

Dynamic routing has a number of different roles routers can fill such as those covered in Dynamic Routing Overview on page 279. BGP has a number of custom roles that routers can fill. These include:

- Speaker routers
- Peer routers or neighbors
- Route reflectors (RR)

Speaker routers

Any router configured for BGP is considered a BGP speaker. This means that a speaker router advertises BGP routes to its peers.

Any routers on the network that are not speaker routers, are not treated as BGP routers.

Peer routers or neighbors

In a BGP network, all neighboring BGP routers or peer routers are routers that are connected to your FortiGate unit. Your FortiGate unit learns about all other routers through these peers.

You need to manually configure BGP peers on your FortiGate unit as neighbors. Otherwise these routers will not be seen as peers, but instead as simply other routers on the network that don't support BGP. You can optionally use MD5 authentication to password protect BGP sessions with those neighbors. (see RFC 2385).

You can configure up to 1000 BGP neighbors on your FortiGate unit. You can clear all or some BGP neighbor connections (sessions) using the `execute router clear bgp` command.

For example, if you have 10 routes in the BGP routing table and you want to clear the specific route to IP address 10.10.10.1, enter the command:

```
execute router clear bgp ip 10.10.10.1
```

To remove all routes for AS number 650001, enter the command:

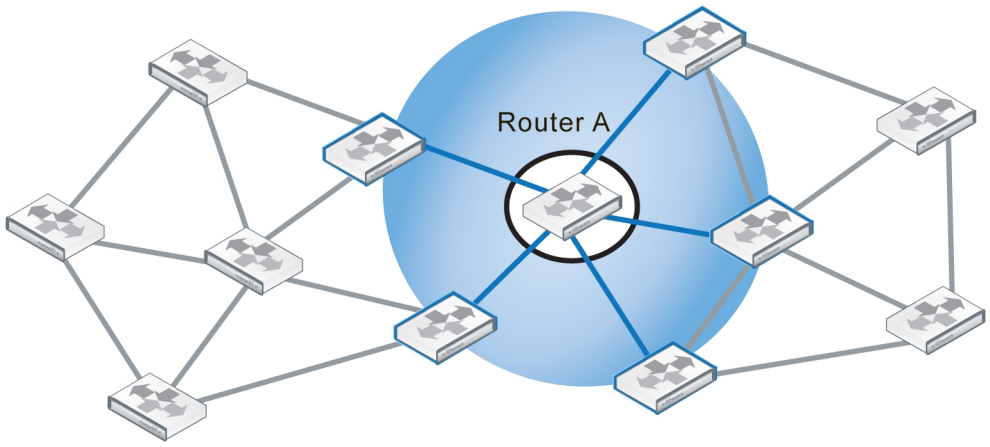
```
execute router clear bgp as 650001
```

To remove route flap dampening information for the 10.10.0.0/16 subnet, enter the command:

```
execute router clear bgp dampening 10.10.0.0/16
```

In Figure 1, Router A is directly connected to five other routers in a network that contains 12 routers overall. These routers, the ones in the blue circle, are Router A's peers or neighbors.

Router A and its 5 peer routers



As a minimum, when configuring BGP neighbors you must enter their IP address, and the AS number (remote-as). This is all the information the web-based manager interface allows you to enter for a neighbor.

The BGP commands related to neighbors are quite extensive and include:

```
config router bgp
```

```
    config neighbor
       edit <neighbor_address_ipv4>
          set activate {enable | disable}
          set advertisement-interval <seconds_integer>
          set allowas-in <max_num_AS_integer>
          set allowas-in-enable {enable | disable}
          set as-override {enable | disable}
          set attribute-unchanged [as-path] [med] [next-hop]
          set bfd {enable | disable}
          set capability-default-originate {enable | disable}
          set capability-dynamic {enable | disable}
          set capability-graceful-restart {enable | disable}
          set capability-orf {both | none | receive | send}
          set capability-route-refresh {enable | disable}
          set connect-timer <seconds_integer>
          set description <text_str>
          set distribute-list-in <access-list-name_str>
          set distribute-list-out <access-list-name_str>
          set dont-capability-negotiate {enable | disable}
          set ebgp-enforce-multihop {enable | disable}
          set ebgp-multihop {enable | disable}
          set ebgp-multihop-ttl <seconds_integer>
          set filter-list-in <aspath-list-name_str>
          set filter-list-out <aspath-list-name_str>
          set holdtime-timer <seconds_integer>
          set interface <interface-name_str>
          set keep-alive-timer <seconds_integer>
          set maximum-prefix <prefix_integer>
          set maximum-prefix-threshold <percentage_integer>
          set maximum-prefix-warning-only {enable | disable}
          set next-hop-self {enable | disable}
          set passive {enable | disable}
          set password <string>
          set prefix-list-in <prefix-list-name_str>
          set prefix-list-out <prefix-list-name_str>
          set remote-as <id_integer>
          set remove-private-as {enable | disable}
          set retain-stale-time <seconds_integer>
          set route-map-in <routemap-name_str>
          set route-map-out <routemap-name_str>
          set route-reflector-client {enable | disable}
          set route-server-client {enable | disable}
          set send-community {both | disable | extended | standard}
          set shutdown {enable | disable}
          set soft-reconfiguration {enable | disable}
          set strict-capability-match {enable | disable}
          set unsuppress-map <route-map-name_str>
          set update-source <interface-name_str>
          set weight <weight_integer>
       end
    end
end
```

Route reflectors (RR)

Route reflectors in BGP concentrate route updates so other routers need only talk to the route reflectors to get all the updates. This results in smaller routing tables, fewer connections between routers, faster responses to network topology changes, and less administration bandwidth. BGP route reflectors are defined in RFC 1966.

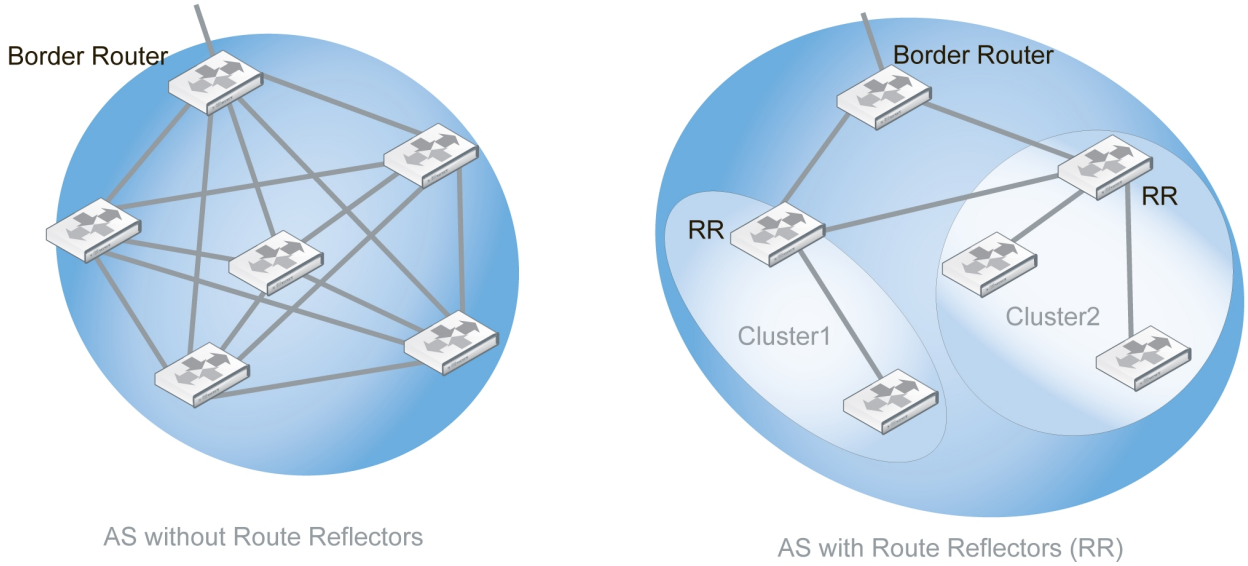
In a BGP route reflector configuration, the AS is divided into different clusters that each include client and reflector routers. The client routers supply the reflector routers with the client's route updates. The reflectors pass this information along to other route reflectors and border routers. Only the reflectors need to be configured, not the clients — the clients will find the closest reflector and communicate with it automatically. The reflectors communicate with each other as peers. FortiGate units can be configured as either reflectors or clients.

Since route reflectors are processing more than the client routers, the reflectors should have more resources to handle the extra workload.

Smaller networks running BGP typically don't require route reflectors (RR). However, RR is a useful feature for large companies, where their AS may include 100 routers or more. For example, for a full mesh 20 router configuration within an AS, there would have to be 190 unique BGP sessions — just for routing updates within the AS. The number of sessions jumps to 435 sessions for just 30 routers, or 4950 sessions for 100 routers. From these numbers, its plain that updating this many sessions will quickly consume the limited bandwidth and processing resources of the routers involved.

The following diagram illustrates how route reflectors can improve the situation when only six routers are involved. The AS without route reflectors requires 15 sessions between the routers. In the AS with route reflectors, the two route reflectors receive route updates from the reflector clients (unlabeled routers in the diagram) in their cluster as well as other route reflectors and pass them on to the border router. The RR configuration only require six sessions. This example shows a reduction of 60% in the number of required sessions.

Required sessions within an AS with and without route reflectors



AS without Route Reflectors

AS with Route Reflectors (RR)

The BGP commands related to route reflectors includes:

```
config router bgp
   config neighbor
```

```
        set route-reflector-client {enable | disable}
        set route-server-client {enable | disable}
    end
end
```

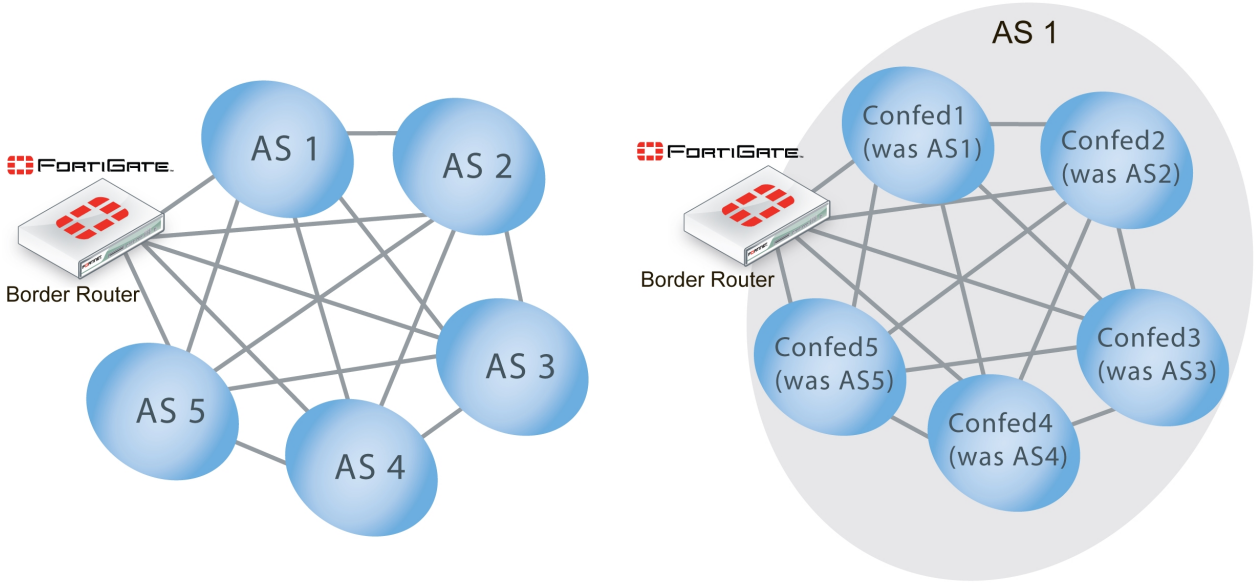
Confederations

Confederations were introduced to reduce the number of BGP advertisements on a segment of the network, and reduce the size of the routing tables. Confederations essentially break up an AS into smaller units. Confederations are defined in RFC 3065 and RFC 1965.

Within a confederation, all routers communicate with each other in a full mesh arrangement. Communications between confederations is more like inter-AS communications in that many of the attributes are changed as they would be for BGP communications leaving the AS, or eBGP.

Confederations are useful when merging ASs. Each AS being merged can easily become a confederation, requiring few changes. Any additional permanent changes can then be implemented over time as required. The figure below shows the group of ASs before merging, and the corresponding confederations afterward as part of the single AS with the addition of a new border router. It should be noted that after merging if the border router becomes a route reflector, then each confederation only needs to communicate with one other router, instead of five others.

AS merging using confederations



Multiple ASes before merging

Combined AS with confederations and new FortiGate unit border router

Confederations and route reflectors perform similar functions — they both sub-divide large ASes for more efficient operation. They differ in that route reflector clusters can include routers that are not members of a cluster, where routers in a confederation must belong to that confederation. Also, confederations place their confederation numbers in the AS_PATH attribute making it easier to trace.

It is important to note that while confederations essentially create sub-ASs, all the confederations within an AS appear as a single AS to external ASs.

Confederation related BGP commands include:

```
config router bgp
   set confederation-identifier <peerid_integer>
end
```

BGP conditional advertisements

Normally, routes are propagated regardless of the existence of a different path. The BGP conditional advertisement feature allows a route not to be advertised based on existence or non-existence of other routes. With this new feature, a child table under bgp.neighbor is introduced. Any route matched by one of the route-map specified in the table will be advertised to the peer based on the corresponding condition route-map.

You can enable and disable conditional advertisements using the CLI.

To configure BGP conditional advertisements - CLI:

```
config router bgp
   set as 3
      config neighbor
         edit "10.10.10.10"
            set remote-as 3
               config conditional-advertise
                  edit "route-map-to-match-sending"
                     set condition-routemap "route-map-to-match-condition"
                     set condition-type [exist | non-exist]
                  next
               end
            next
         end
```

BGP Neighbor Groups

The BGP Neighbor Groups feature allows a large number of neighbors to be configured automatically based on a range of neighbors' source addresses.

To configure BGP Neighbor Groups - CLI:

Start by adding a BGP neighbor group:

```
config router bgp
   config neighbor-group
      edit <neighbor-group-name>
         set remote-as 100
   ...
```

(All options for BGP neighbor are supported except `password`.)

```
end
```

Then add a BGP neighbor range:

```
config router bgp
   config neighbor-range
      edit 1
         set prefix 192.168.1.0/24
         set max-neighbor-num 100
         set neighbor-group <neighbor-group-name>
      next
```

```
end
```

Network Layer Reachability Information (NLRI)

Network Layer Reachability Information (NLRI) is unique to BGP-4. It is sent as part of the update messages sent between BGP routers, and contains information necessary to supernet, or aggregate route, information. The NLRI includes the length and prefix that when combined are the address of the aggregated routes referred to.

There is only one NLRI entry per BGP update message.

BGP attributes

Each route in a BGP network has a set of attributes associated with it. These attributes define the route, and are modified as required along the route.

BGP can work well with mostly default settings, but if you are going to change settings you need to understand the roles of each attribute and how they affect those settings.

The BGP attributes include:

AS_PATH	A list of ASes a route has passed through. See AS_PATH on page 339.
MULTI_EXIT_DESC (MED)	Which router to use to exit an AS with more than one external connection. See MULTI_EXIT_DESC (MED) on page 340.
COMMUNITY	Used to apply attributes to a group of routes. See COMMUNITY on page 341.
NEXT_HOP	Where the IP packets should be forwarded to, like a gateway in static routing. See NEXT_HOP on page 341.
ATOMIC_AGGREGATE	Used when routes have been summarized to tell downstream routers not to de-aggregate the route. See ATOMIC_AGGREGATE on page 341.
ORIGIN	Used to determine if the route is from the local AS or not. See ORIGIN on page 342.
LOCAL_PREF	Used only within an AS to select the best route to a location (like MED)

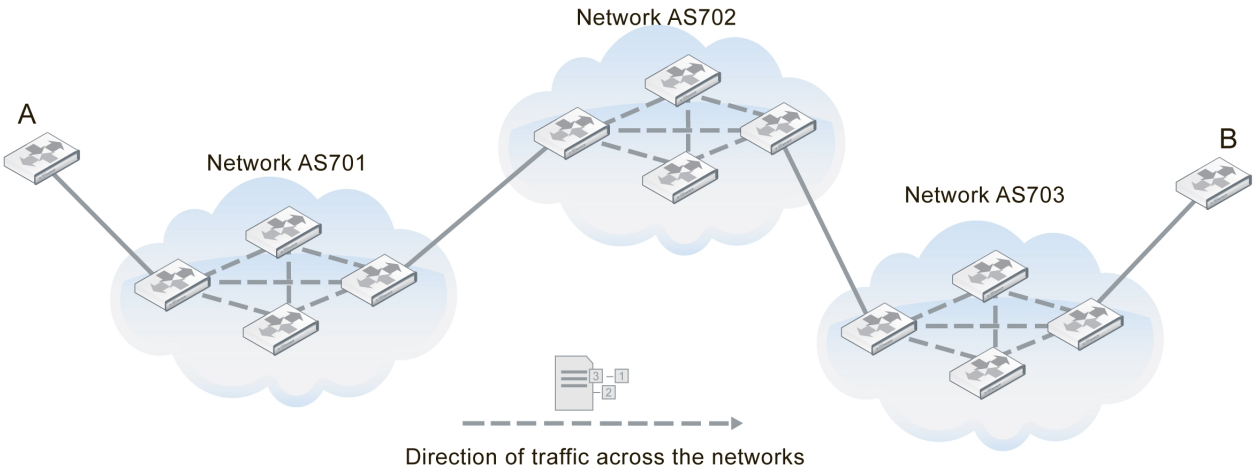
Inbound policies on FortiGate units can change the NEXT-HOP,LOCAL-PREF, MED and AS-PATH attributes of an internal BGP (iBGP) route for its local route selection purposes. However, outbound policies on the unit cannot affect these attributes.

AS_PATH

AS_PATH is the BGP attribute that keeps track of each AS a route advertisement has passed through. AS_PATH is used by confederations and by exterior BGP (EBGP) to help prevent routing loops. A router knows there is a loop if it receives an AS_PATH with that routers AS in it. The figure below shows the route between router A and router B. The AS_PATH from A to B would read 701,702,703 for each AS the route passes through.

As of the start of 2010, the industry upgraded from 2-byte to 4-byte AS_PATHs. This upgrade was due to the imminent exhaustion of 2-byte AS_PATH numbers. FortiOS supports 4-byte AS_PATHs in its BGP implementation.

AS_PATH of 701,702, 703 between routers A and B



The BGP commands related to AS_PATH include:

```
config router bgp
   set bestpath-as-path-ignore {enable | disable}
end
```

MULTI_EXIT_DESC (MED)

BGP AS systems can have one or more routers that connect them to other ASes. For ASes with more than one connecting router, the Multi-Exit Discriminator (MED) lists which router is best to use when leaving the AS. The MED is based on attributes such as delay. It is a recommendation only, as some networks may have different priorities.

BGP updates advertise the best path to a destination network. When the FortiGate unit receives a BGP update, the FortiGate unit examines the Multi-Exit Discriminator (MED) attribute of potential routes to determine the best path to a destination network before recording the path in the local FortiGate unit routing table.

FortiGate units have the option to treat any routes without an MED attribute as the worst possible routing choice. This can be useful because a lack of MED information is a lack of routing information which can be suspicious — possibly a hacking attempt or an attack on the network. At best it signifies an unreliable route to select.

The BGP commands related to MED include:

```
config router bgp
   set always-compare-med {enable | disable}
   set bestpath-med-confed {enable | disable}
   set bestpath-med-missing-as-worst {enable | disable}
   set deterministic-med {enable | disable}
   config neighbor
      set attribute-unchanged [as-path] [med] [next-hop]
   end
end
```

COMMUNITY

A community is a group of routes that have the same routing policies applied to them. This saves time and resources. A community is defined by the COMMUNITY attribute of a BGP route.

The FortiGate unit can set the COMMUNITY attribute of a route to assign the route to predefined paths (see RFC 1997). The FortiGate unit can examine the COMMUNITY attribute of learned routes to perform local filtering and/or redistribution.

The BGP commands related to COMMUNITY include:

```
config router bgp
   set send-community {both | disable | extended | standard}
end
```

NEXT_HOP

The NEXT_HOP attribute says what IP address the packets should be forwarded to next. Each time the route is advertised, this value is updated. The NEXT_HOP attribute is much like a gateway in static routing.

FortiGate units allow you to to change the advertising of the FortiGate unit's IP address (instead of the neighbor's IP address) in the NEXT_HOP information that is sent to IBGP peers. This is changed with the config neighbor, set next-hop-self command.

The BGP commands related to NEXT_HOP include:

```
config router bgp
   config neighbor
      set attribute-unchanged [as-path] [med] [next-hop]
      set next-hop-self {enable | disable}
   end
end
```

ATOMIC_AGGREGATE

The ATOMIC_AGGREGATE attribute is used when routes have been summarized. It indicates which AS and which router summarize the routes. It also tells downstream routers not to de-aggregate the route. Summarized routes are routes with similar information that have been combined, or aggregated, into one route that is easier to send in updates. When it reaches its destination, the summarized routes are split back up into the individual routes.

Your FortiGate unit doesn't specifically set this attribute in the BGP router command, but it is used in the route map command.

The commands related to ATOMIC_AGGREGATE include:

```
config router route-map
   edit <route_map_name>
      config rule
      edit <route_map_rule_id>
         set set-aggregator-as <id_integer>
         set set-aggregator-ip <address_ipv4>
         set set-atomic-aggregate {enable | disable}
      end
   end
end
```

ORIGIN

The ORIGIN attribute records where the route came from. The options can be IBGP, EBGP, or incomplete. This information is important because internal routes (IBGP) are by default higher priority than external routes (EBGP). However incomplete ORIGINs are the lowest priority of the three.

The commands related to ORIGIN include:

```
config router route-map
   edit <route_map_name>
      set comments <string>
      config rule
      edit <route_map_rule_id>
         set match-origin {egp | igp | incomplete | none}
      end
   end
end
```

How BGP works

BGP is a link-state routing protocol and keeps link-state information about the status of each network link it has connected. A BGP router receives information from its peer routers that have been defined as neighbors. BGP routers listen for updates from these configured neighboring routers on TCP port 179.

A BGP router is a finite state machine with six various states for each connection. As two BGP routers discover each other, and establish a connection they go from the idle state, through the various states until they reach the established state. An error can cause the connection to be dropped and the state of the router to be reset to either active or idle. These errors can be caused by: TCP port 179 not being open, a random TCP port above port 1023 not being open, the peer address being incorrect, or the AS number being incorrect.

When BGP routers start a connection, they negotiate which (if any) optional features will be used such as multiprotocol extensions that can include IPv6 and VPNs.

IBGP versus EBGP

When you read about BGP, often you see EBGP or IBGP mentioned. These are both BGP routing, but BGP used in different roles. Exterior BGP (EBGP) involves packets crossing multiple autonomous systems (ASes) where interior BGP (IBGP) involves packets that stay within a single AS. For example the AS_PATH attribute is only useful for EBGP where routes pass through multiple ASes.

These two modes are important because some features of BGP are only used for one of EBGP or IBGP. For example confederations are used in EBGP, and route reflectors are only used in IBGP. Also routes learned from IBGP have priority over EBGP learned routes.

FortiGate units have some commands specific to EBGP. These include:

- automatically resetting the session information to external peers if the connection goes down — `set fast-external-failover {enable | disable}`
- setting an administrative distance for all routes learned from external peers (must also configure local and internal distances if this is set) — `set distance-external <distance_integer>`
- enforcing EBGP multihops and their TTL (number of hops) — `set ebgp-enforce-multihop {enable | disable}` and `set ebgp-multihop-ttl <seconds_integer>`

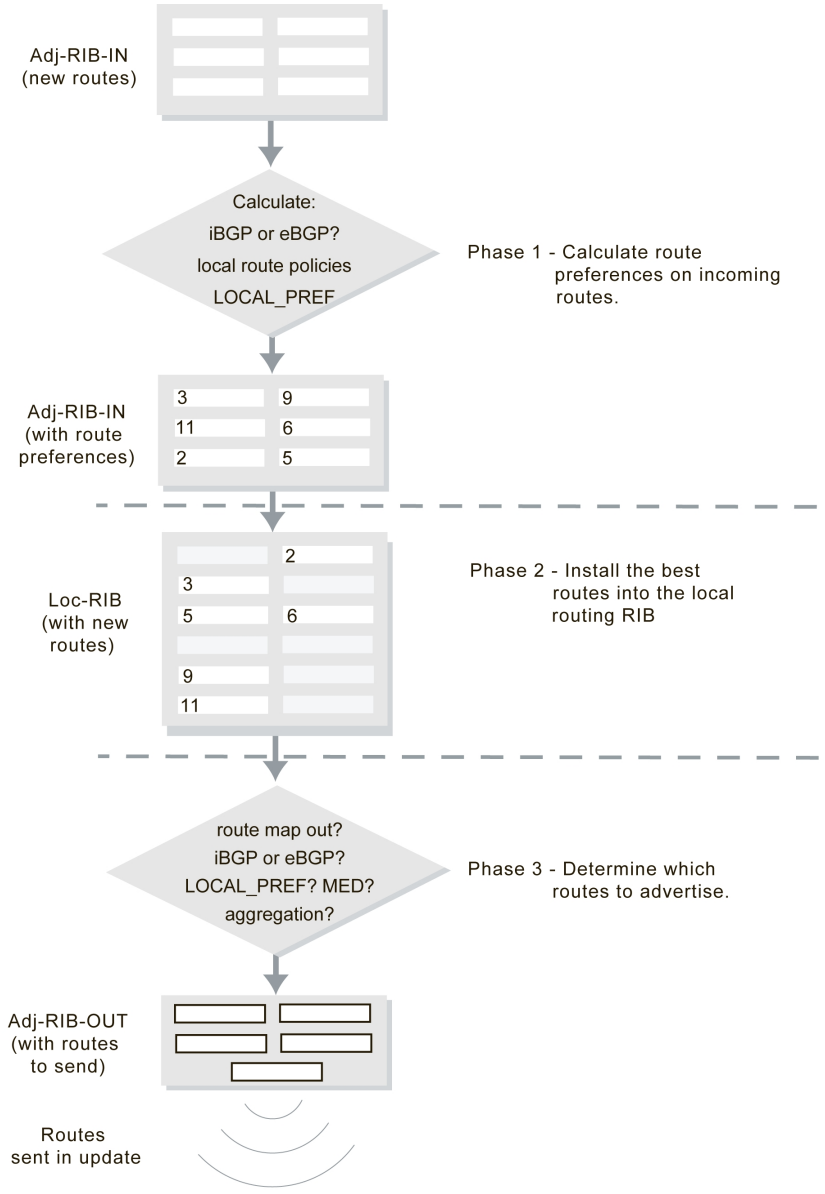
BGP path determination — which route to use

Firstly, recall that the number of available or supported routes is not set by the configuration but depends on your FortiGate's available memory. All learned routes and their attributes come into the BGP router in raw form. Before routes are installed in the routing table or are advertised to other routers, three levels of decisions must be made.

The three phases of BGP best path determination do not change. However, some manufacturers have added more information to the process, such as Cisco's WEIGHT attribute to enable an administrator to force one route's selection over another.

There is one Adj-RIB-IN and Adj-RIB-OUT for each configured neighbor. They are updated when the FortiGate unit receives BGP updates, or when the FortiGate unit sends out BGP updates.

Three phases of BGP routing decision



Decision phase 1

At this phase, the decision is to calculate how preferred each route and its NRLI are the Adjacent Routing Information Base Incoming (Adj-RIBs-In) compared to the other routes. For internal routes (IBGP), policy information or LOCAL_PREF is used. For external peer learned routes, it is based strictly on policy. These rules set up a list of which routes are most preferred going into Phase 2.

Decision phase 2

Phase 2 involves installing the best route to each destination into the local Routing Information Base (Loc-RIB). Effectively, the Loc-RIB is the master routing table. Each route from Phase 1 has their NEXT_HOP checked to

ensure the destination is reachable. If it is reachable, the AS_PATH is checked for loops. After that, routes are installed based on the following decision process:

- If there is only one route to a location, it is installed.
- If multiple routes to the same location, use the most preferred route from Level 1.
- If there is a tie, break the tie based on the following in descending order of importance: shortest AS_PATH, smallest ORIGIN number, smallest MED, EBGP over IBGP, smallest metric or cost for reaching the NEXT_HOP, BGP identifier, and lowest IP address.

Note that the new routes that are installed into the Loc-RIB are in addition to any existing routes in the table. Once Phase 2 is completed the Loc-RIB will consist of the best of both the new and older routes.

Decision phase 3

Phase 3 is route distribution or dissemination. This is the process of deciding which routes the router will advertise. If there is any route aggregation or summarizing, it happens here. Also any route filtering from route maps happens here.

Once Phase 3 is complete, an update can be sent out to update the neighbor of new routes.

Aggregate routes and addresses

BGP4 allows classless routing, which uses netmasks as well as IP addresses. This classless routing enables the configuration of aggregate routes by stating the address bits the aggregated addresses have in common. For more information, see Dynamic Routing Overview on page 279.

The ATOMIC_AGGREGATE attribute informs routers that the route has been aggregated, and should not be de-aggregated. An associated AGGREGATOR attribute include the information about the router that did the aggregating including its AS.

The BGP commands associated with aggregate routes and addresses are:

```
config router bgp
   config aggregate-address
      edit <aggr_addr_id>
      set as-set {enable | disable}
      set prefix <address_ipv4mask>
      set summary-only {enable | disable}
   end
   config aggregate-address6
      edit <aggr_addr_id>
      set as-set {enable | disable}
      set prefix6 <address_ipv6mask>
      set summary-only {enable | disable}
   end
```

Troubleshooting BGP

There are some features in BGP that are used to deal with problems that may arise. Typically the problems with a BGP network that has been configured, involve routes going offline frequently. This is called route flap and causes problems for the routers using that route.

Clearing routing table entries

To see if a new route is being properly added to the routing table, you can clear all or some BGP neighbor connections (sessions) using the `execute router clear bgp` command.

For example, if you have 10 routes in the BGP routing table and you want to clear the specific route to IP address 10.10.10.1, enter the command:

```
execute router clear bgp ip 10.10.10.1
```

To remove all routes for AS number 650001, enter the command:

```
execute router clear bgp as 650001
```

Route flap

When routers or hardware along a route go offline and back online that is called a route flap. Flapping is the term if these outages continue, especially if they occur frequently.

Route flap is a problem in BGP because each time a peer or a route goes down, all the peer routers that are connected to that out-of-service router advertise the change in their routing tables which creates a lot of administration traffic on the network. And the same traffic happens again when that router comes back online. If the problem is something like a faulty network cable that wobbles on and offline every 10 seconds, there could easily be overwhelming amounts of routing updates sent out unnecessarily.

Another possible reason for route flap occurs with multiple FortiGate units in HA mode. When an HA cluster fails over to the secondary unit, other routers on the network may see the HA cluster as being offline resulting in route flap. While this doesn't occur often, or more than once at a time, it can still result in an interruption in traffic which is unpleasant for network users. The easy solution for this problem is to increase the timers on the HA cluster, such as TTL timers, so they do not expire during the failover process. Also configuring graceful restart on the HA cluster will help with a smooth failover.

The first method of dealing with route flap should be to check your hardware. If a cable is loose or bad, it can easily be replaced and eliminate the problem. If an interface on the router is bad, either avoid using that interface or swap in a functioning router. If the power source is bad on a router, either replace the power supply or use a power conditioning backup power supply. These quick and easy fixes can save you from configuring more complex BGP options. However if the route flap is from another source, configuring BGP to deal with the outages will ensure your network users uninterrupted service.

Some methods of dealing with route flap in BGP include:

- Holddown timer
- Dampening
- Graceful restart
- Bi-directional forwarding detection (BFD)

Holddown timer

The first line of defence to a flapping route is the hold down timer. This timer reduces how frequently a route going down will cause a routing update to be broadcast.

Once activated, the holddown timer won't allow the FortiGate unit to accept any changes to that route for the duration of the timer. If the route flaps five times during the timer period, only the first outage will be recognized by the FortiGate unit — for the duration of the other outages there will be no changes because the Fortigate unit is essentially treating this router as down. After the timer expires, if the route is still flapping it will happen all over again.

Even if the route isn't flapping — if it goes down, comes up, and stays back up — the timer still counts down and the route is ignored for the duration of the timer. In this situation the route will be seen as down longer than it really is, but there will be only the one set of route updates. This is not a problem in normal operation because updates are not frequent.

Also the potential for a route to be treated as down when it is really up can be viewed as a robustness feature. Typically you do not want most of your traffic being routed over an unreliable route. So if there is route flap going on, it is best to avoid that route if you can. This is enforced by the holddown timer.

How to configure the holddown timer

There are three different route flapping situations that can occur: the route goes up and down frequently, the route goes down and back up once over a long period of time, or the route goes down and stays down for a long period of time. These can all be handled using the holddown timer.

For example, your network has two routes that you want to set the holddown timer for. One is your main route (to 10.12.101.4) that all your Internet traffic goes through, and it can't be down for long if its down. The second is a low speed connection to a custom network that is used infrequently (to 10.13.101.4). The holddown timer for the main route should be fairly short, lets say 60 seconds instead of the default 180 seconds. The second route timer can be left at the default or even longer since it is rarely used. In your BGP configuration this looks like:

```
config router bgp
   config neighbor
   edit 10.12.101.4
      set holddown-timer 60
   next
   edit 10.13.101.4
      set holddown-timer 180
   next
   end
end
```

Dampening

Dampening is a method used to limit the amount of network problems due to flapping routes. With dampening the flapping still occurs, but the peer routers pay less and less attention to that route as it flaps more often. One flap doesn't start dampening, but the second starts a timer where the router will not use that route — it is considered unstable. If the route flaps again before the timer expires, the timer continues to increase. There is a period of time called the reachability half-life after which a route flap will only be suppressed for half the time. This half-life comes into effect when a route has been stable for a while but not long enough to clear all the dampening completely. For the flapping route to be included in the routing table again, the suppression time must expire.

If the route flapping was temporary, you can clear the flapping or dampening from the FortiGate units cache by using one of the `execute router clear bgp` commands:

```
execute router clear bgp dampening {<ip_address> | <ip/netmask>}
```
or
```
execute router clear bgp flap-statistics {<ip> | <ip/netmask>}
```

For example, to remove route flap dampening information for the 10.10.0.0/16 subnet, enter the command:

```
execute router clear bgp dampening 10.10.0.0/16
```

The BGP commands related to route dampening are:

```
config router bgp
   set dampening {enable | disable}
```

```
    set dampening-max-suppress-time <minutes_integer>
    set dampening-reachability-half-life <minutes_integer>
    set dampening-reuse <reuse_integer>
    set dampening-route-map <routemap-name_str>
    set dampening-suppress <limit_integer>
    set dampening-unreachability-half-life <minutes_integer>
end
```

Graceful restart

BGP4 has the capability to gracefully restart.

In some situations, route flap is caused by routers that appear to be offline but the hardware portion of the router (control plane) can continue to function normally. One example of this is when some software is restarting or being upgraded, but the hardware can still function normally.

Graceful restart is best used for these situations where routing will not be interrupted, but the router is unresponsive to routing update advertisements. Graceful restart does not have to be supported by all routers in a network, but the network will benefit when more routers support it.

FortiGate HA clusters can benefit from graceful restart. When a failover takes place, the HA cluster will advertise it is going offline, and will not appear as a route flap. It will also enable the new HA main unit to come online with an updated and usable routing table — if there is a flap the HA cluster routing table will be out of date.

For example, your FortiGate unit is one of four BGP routers that send updates to each other. Any of those routers may support graceful starting—when a router plans to go offline, it will send out a message to its neighbors how long it expects to be before being back online. That way its neighbor routers don't remove it from their routing tables. However if that router isn't back online when expected, the routers will mark it offline. This prevents routing flap and its associated problems.

Scheduled time offline

Graceful restart is a means for a router to advertise it is going to have a scheduled shutdown for a very short period of time. When neighboring routers receive this notice, they will not remove that router from their routing table until after a set time elapses. During that time if the router comes back online, everything continues to function as normal. If that router remains offline longer than expected, then the neighboring routers will update their routing tables as they assume that router will be offline for a long time.

FortiGate units support both graceful restart of their own BGP routing software, and also neighboring BGP routers.

For example, if a neighbor of your FortiGate unit, with an IP address of 172.20.120.120, supports graceful restart, enter the command:

```
config router bgp
   config neighbor
   edit 172.20.120.120
      set capability-graceful-restart enable
   end
end
```

If you want to configure graceful restart on your FortiGate unit where you expect the Fortigate unit to be offline for no more than 2 minutes, and after 3 minutes the BGP network should consider the FortiGate unit offline, enter the command:

```
config router bgp
   set graceful-restart enable
   set graceful-restart-time 120
   set graceful-stalepath-time 180
end
```

The BGP commands related to BGP graceful restart are:

```
config router bgp
   set graceful-restart { disable| enable}
   set graceful-restart-time <seconds_integer>
   set graceful-stalepath-time <seconds_integer>
   set graceful-update-delay <seconds_integer>
   config neighbor
      set capability-graceful-restart {enable | disable}
   end
end

execute router restart
```

Before the restart, the router sends its peers a message to say it is restarting. The peers mark all the restarting router's routes as stale, but they continue to use the routes. The peers assume the router will restart and check its routes and take care of them if needed after the restart is complete. The peers also know what services the restarting router can maintain during its restart. After the router completes the restart, the router sends its peers a message to say it is done restarting.

Bi-directional forwarding detection (BFD)

Bi-directional Forwarding Detection (BFD) is a protocol used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated.

While BGP can detect route failures, BFD can be configured to detect these failures more quickly allowing faster responses and improved convergence. This can be balanced with the bandwidth BFD uses in its frequent route checking.

Configurable granularity

BFD can run on the entire FortiGate unit, selected interfaces, or on BGP for all configured interfaces. The hierarchy allows each lower level to override the upper level's BFD setting. For example, if BFD was enabled for the FortiGate unit, it could be disabled only for a single interface or for BGP. For information about FortiGate-wide BFD options, see config system settings in the FortiGate CLI Reference.

BFD can only be configured through the CLI.

The BGP commands related to BFD are:

```
config system {setting | interface}
   set bfd {enable | disable | global}
   set bfd-desired-mix-tx <milliseconds>
   set bfd-detect-mult <multiplier>
   set bfd-required-mix-rx <milliseconds>
   set bfd-dont-enforce-src-port {enable | disable}

config router bgp
   config neighbor
      edit <neighbor_address_ipv4>
```

```
        set bfd {enable | disable}
    end
end

get router info bfd neighbor
execute router clear bfd session <src_ipv4> <dst_ipv4> <interface>
```

The `config system` commands allow you to configure whether BFD is enabled in a particular unit/vdom or individual interface, and how often the interface requires sending and receiving of BFD information.

The `config router bgp` commands allow you to set the addresses of the neighbor units that are also running BFD. Both units must be configured with BFD in order to make use of it.

Dual-homed BGP example

This is an example of a small network that uses BGP routing connections to two ISPs. This is a common configuration for companies that need redundant connections to the Internet for their business.

This configuration is for a small company connected to two ISPs. The company has one main office, the Head Office, and uses static routing for internal routing on that network.

Both ISPs use BGP routing, and connect to the Internet directly. They want the company to connect to the ISP networks using BGP. They also use graceful restart to prevent unneeded updates, and use smaller timer values to detect network failures faster.

As can be expected, the company wants to keep their BGP configuration relatively simple and easy to manage. The current configuration has only 3 routers to worry about — the 2 ISP border routers, and the FortiGate unit. This means the FortiGate unit will only have two neighbor routers to configure.

This configuration has the added benefit of being easy to expand if the Company wants to add a remote office in the future.

To keep the configuration simple, the Company is allowing only HTTP, HTTPS, FTP, and DNS traffic out of the local network. This will allow employees access to the Internet and their web-mail.

This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate unit
- Configuring other networking devices
- Testing this configuration

Why dual home?

Dual homing means having two separate independent connections to the Internet. Servers in this configuration have also been called bastion hosts and can include DNS servers which require multiple connections.

Benefits of dual homing can include:

- Redundant Internet connection that essentially never fails
- Faster connections through one ISP or the other for some destinations, such as other clients of those ISPs
- Load balancing traffic to your Company network
- Easier to enable more traffic through two connections than upgrading one connection to bigger bandwidth
- Easier to create protection policies for different traffic through a specific ISP

Some companies require reliable Internet access at all times as part of their business. Consider a doctor operating remotely who has their Internet connection fail — the consequences could easily be life or death.

Dual homing is extra expense for the second ISP connection, and more work to configure and maintain the more complex network topology.

Potential dual homing issues

BGP comes with load balancing issues, and dual homing is the same category. BGP does not inherently deal well with load balancing, or getting default routes through BGP. Ideally one connect may be best for certain destinations, but it may not have that traffic routed to it making the load balancing less than perfect. This kind of fine tuning can be very time consuming, and usually results in a best effort situation.

When dual homing is not configured properly, your network may become a link between your ISPs and result in very high traffic between the ISPs that does not originate from your network. The problems with this situation are that your traffic may not have the bandwidth it needs, and you will be paying for a large volume of traffic that is not yours. This problem can be solved by not broadcasting or redistributing BGP routes between the ISPs.

If you learn your default routes from the ISPs in this example, you may run into an asymmetric routing problem where your traffic loops out one ISP and back to you through the other ISP. If you think this may be happening you can turn on asymmetric routing on the FortiGate unit (config system settings, set asymmetric enable) to verify that really is the problem. Turn this feature off once this is established since it disables many features on the FortiGate by disabling stateful inspection. Solutions for this problem can include using static routes for default routes instead of learning them through BGP, or configuring VDOMs on your FortiGate unit to provide a slightly different path back that is not a true loop.

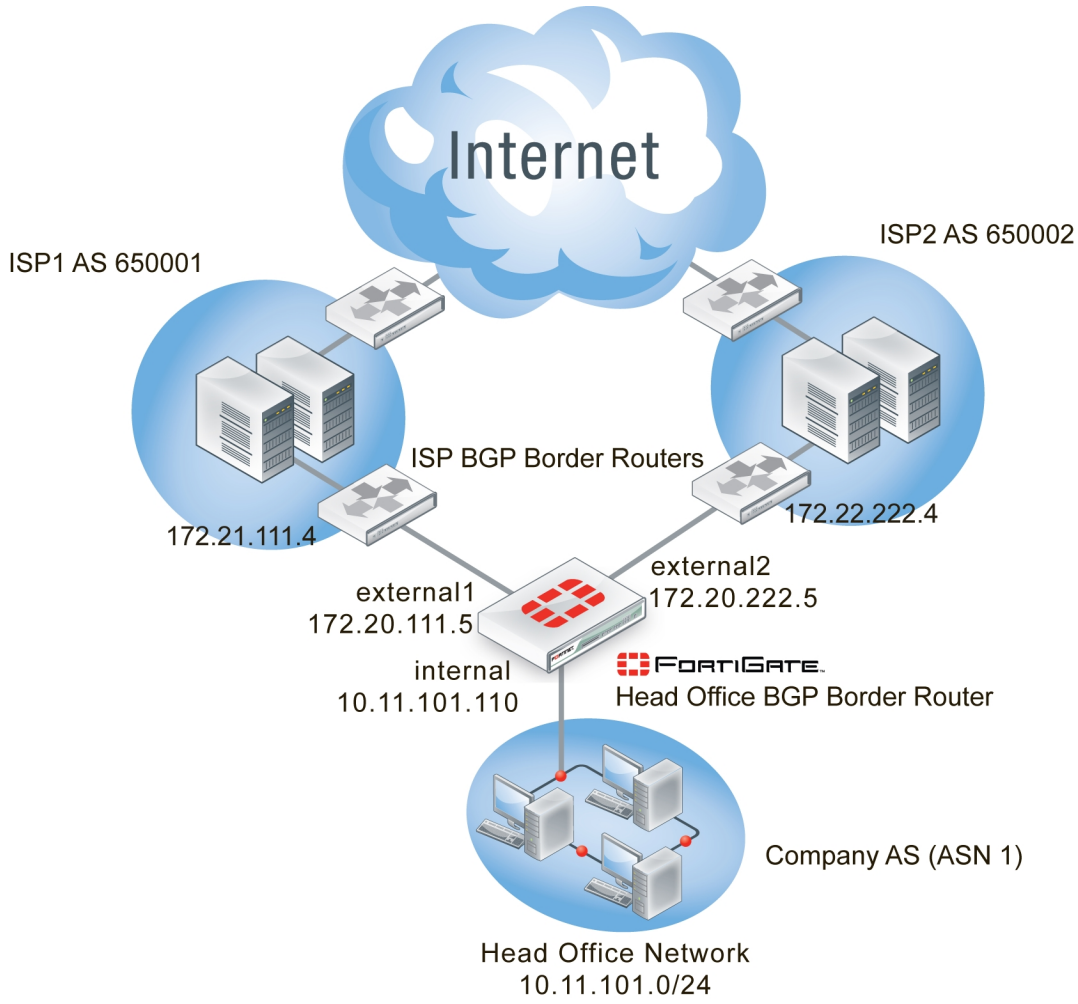
Network layout and assumptions

The network layout for the basic BGP example involves the company network being connected to both ISPs as shown below. In this configuration the FortiGate unit is the BGP border router between the Company AS, ISP1's AS, and ISP2's AS.

The components of the layout include:

- The Company AS (AS number 1) is connected to ISP1 and ISP2 through the FortiGate unit.
- The Company has one internal network — the Head Office network at 10.11.101.0/24.
- The FortiGate unit internal interface is on the the Company internal network with an IP address of 10.11.101.110.
- The FortiGate unit external1 interface is connected to ISP1's network with an IP address of 172.20.111.5, an address supplied by the ISP.
- The FortiGate unit external2 interface is connected to IPS2's network with an IP address of 172.20.222.5, an address supplied by the ISP.
- ISP1 AS has an AS number of 650001, and ISP2 has an AS number of 650002.
- Both ISPs are connected to the Internet.
- The ISP1 border router is a neighbor (peer) of the FortiGate unit. It has an address of 172.21.111.4.
- The ISP2 border router is a neighbor (peer) of the FortiGate unit. It has an address of 172.22.222.4.
- Apart from graceful restart, and shorter timers (holdtimer, and keepalive) default settings are to be used whenever possible.

Basic BGP network topology



Assumptions

The basic BGP configuration procedure follows these assumptions:

- ISP1 is the preferred route, and ISP2 is the secondary route
- All basic configuration can be completed in both GUI and CLI
- Only one AS is used for the Company

For these reasons this example configuration does not include:

- Bi-directional forwarding detection (BFD)
- Route maps
- Access lists
- Changing redistribution defaults — make link when example is set up
- IPv6

For more information on these features, see the corresponding section.

Configuring the FortiGate unit

In this topology, the FortiGate unit is the link between the Company Network and the ISP network. The FortiGate unit is the only BGP router on the Company Network, but there is at least one other BGP router on the ISP Network — there may be more but we don't have that information.

As mentioned in the general configuration steps, the ISP must be notified of the Company's BGP router configuration when complete as it will need to add the FortiGate BGP router as a neighbor router on its domain. This step is required for the FortiGate unit to receive BGP routing updates from the ISP network and outside networks.

If the ISP has any special BGP features enabled such as graceful restart, or route dampening that should be determined up front so those features can be enabled on the FortiGate unit.

To configure the FortiGate unit as a BGP router

1. Configure interfaces and default routes
2. Configure firewall services, addresses, and policies
3. Set the FortiGate BGP information
4. Add the internal network to the AS
5. Additional FortiGate BGP configuration

Configure interfaces and default routes

The FortiGate unit is connected to three networks — Company Network on the internal interface, ISP1 Network on external1interface, and ISP2 on external2 interface.

This example uses basic interface settings. Check with your ISP to determine if additional settings are required such as setting the maximum MTU size, or if gateway detection is supported.

High end FortiGate units do not have interfaces labeled Internal, or External. Instead, for clarity's sake, we are using the alias feature to name interfaces for these roles.

Default routes to both external interfaces are configured here as well. Both are needed in case one goes offline. ISP1 is the primary connection and has a smaller administrative distance so it will be preferred over ISP2. Both distances are set low so they will be preferred over any learned routes.

To configure the FortiGate interfaces - web-based manager

1. Go to **System > Network > Interface**.
2. Edit port 1 (internal) interface.
3. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.110/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Company internal network
Administrative Status	Up

4. Edit port 2 (external1) interface.
5. Set the following information, and select **OK**.

Alias	external1
IP/Network Mask	172.21.111.5/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	ISP1 External BGP network
Administrative Status	Up

6. Edit port 3 (external2) interface.
7. Set the following information, and select **OK**.

Alias	external2
IP/Network Mask	172.22.222.5/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	ISP2 External BGP network
Administrative Status	Up

To configure the FortiGate interfaces - CLI

```
config system interface
   edit port1
      set alias internal
      set ip 10.11.101.110 255.255.255.0
      set allowaccess http https ssh
      set description "Company internal network"
      set status up
   next
   edit port2
      set alias external1
      set ip 172.21.111.5 255.255.255.0
      set allowaccess https ssh
      set description "ISP1 External BGP network"
      set status up
   next
   edit port3
      set alias external2
      set ip 172.22.222.5 255.255.255.0
      set allowaccess https ssh
      set description "ISP2 External BGP network"
      set status up
   next
end
```

To configure default routes for both ISPs - web-based manager

1. Go to **Router > Static > Static Routes**.
2. Delete any existing routes with a IP/Mask of address of 0.0.0.0/0.0.0.0
3. Select **Create New**, and set the following information.

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2
Gateway	172.21.111.5
Distance	10

4. Select **OK**.
5. Select **Create New**, and set the following information.

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3
Gateway	172.22.222.5
Distance	15

6. Select **OK**.

To configure default routes for both ISPs - CLI

```
config router static
   edit 1
      set device "port2"
      set distance 10
      set gateway 172.21.111.5
   next
   edit 2
      set device "port3"
      set distance 15
      set gateway 172.22.222.5
   next
end
```

Configure firewall services, addresses, and policies

To create the security policies, first you must create the firewall services group that will include all the services that will be allowed, then you must define the addresses that will be used in the security policies, and lastly you configure the security policies themselves.

To keep the configuration simple, the Company is allowing only HTTP traffic out of the local network. This will allow employees access to the Internet and their web-mail. DNS services will also be allowed through the firewall.

The security policies will allow HTTP traffic (port 80 and port 8080), HTTPS traffic (port 443), FTP traffic (port 21), and DNS traffic (port 53 and port 953) in both directions. Also BGP (port 179) may need access through the firewall.

For added security, you may want to define a smaller range of addresses for the internal network. For example if only 20 addresses are used, only allow those addresses in the range.

In the interest of keeping things simple, a zone will be used to group the two ISP interfaces together. This will allow using one security policy to apply to both ISPs at the same time. Remember to block intra-zone traffic as this will help prevent one ISP sending traffic to the other ISP through your FortiGate unit using your bandwidth. The zone keeps configuration simple, and in the future if there is a need for separate policies for each ISP, they can be created and the zone can be deleted.

The addresses that will be used are the addresses of the FortiGate unit internal and external ports, and the internal network.

More policies or services can be added in the future as applications are added to the network. For more information on security policies, see the firewall chapter of the FortiGate Administration Guide.

When configuring security policies always enable logging to help you track and debug your traffic flow.

To create a firewall services group - web-based manager

1. Go to **Policy & Objects > Objects > Services**, select the dropdown arrow next to **Create New** and select **Service Group**.
2. For **Group Name**, enter “Basic_Services”.
3. From the **Members** dropdown, choose the following six services — BGP, FTP, FTP_GET, FTP_PUT, DNS, HTTP, and HTTPS.
4. Select **OK**.

To create a firewall services group - CLI

```
config firewall service group
   edit "Basic_Services"
      set member "BGP" "DNS" "FTP" "FTP_GET" "FTP_PUT" "HTTP" "HTTPS"
   next
end
```

To create a zone for the ISP interfaces - web-based manager

1. Go to **System > Network > Interfaces.**
2. Select the caret to the right of **Create New** and then select **Zone**.
3. Enter the following information.

Zone Name	ISPs
Block Intra-zone traffic	enable
interface members	port2 port3

4. Select **OK**.

To create a zone for the ISP interfaces - CLI

```
config system zone
   edit "ISPs"
      set interface "port2" "port3"
      set intrazone block
   next
end
```

To add the firewall addresses - web-based manager

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, and set the following information.

Category	Address
Name	Internal_network
Type	Subnet / IP Range
Subnet / IP Range	10.11.101.0 255.255.255.0
Interface	port1

3. Select **OK**.

To add the firewall addresses - CLI

```
config firewall address
   edit "Internal_network"
      set associated-interface "port1"
      set subnet 10.11.101.0 255.255.255.0
   next
end
```

To add the HTTP and DNS security policies - web-based manager

1. Go to **Policy & Objects > Policy > IPv4**, and select **Create New**.
2. Set the following information.

Incoming Interface	port1(internal)
Source Address	Internal_network
Outgoing Interface	ISPs
Destination Address	All
Schedule	Always
Service	Basic_services
Action	ACCEPT

Log Allowed Traffic	Enable
Firewall / Network Options	Enable NAT
Comments	ISP1 basic services out policy

3. Select **OK**.
4. Select **Create New**, and set the following information.

Incoming Interface	ISPs
Source Address	All
Outgoing Interface	port1(internal)
Destination Address	Internal_network
Schedule	Always
Service	Basic_services
Action	ACCEPT
Log Allowed Traffic	Enable
Firewall / Network Options	Enable NAT
Comments	ISP1 basic services in policy

To add the security policies - CLI

```
config firewall policy
   edit 1
      set srcintf "port1"
      set srcaddr "Internal_network"
      set dstintf "ISPs"
      set dstaddr "all"
      set schedule "always"
      set service "Basic_services"
      set action accept
      set nat enable
      set profile-status enable
      set logtraffic enable
      set comments "ISP1 basic services out policy"
   next
   edit 2
      set srcintf "ISPs"
      set srcaddr "all"
      set dstintf "port1"
      set dstaddr "Internal_network"
      set schedule "always"
      set service "Basic_services"
      set action accept
      set nat enable
      set profile-status enable
      set logtraffic enable
```

```
      set comments "ISP1 basic services in policy"
   next
end
```

Set the FortiGate BGP information

When using the default information, there are only two fields to set to configure the FortiGate unit as a BGP router.

For this configuration the FortiGate unit will be in a stub area with one route out — the ISP BGP router. Until you configure the ISP router as a neighbor, even that route out is not available. So while after this part of the configuration is complete your FortiGate unit will be running BGP, it won't know about any other routers running BGP until the next part of the configuration is complete.

To set the BGP router information - web-based mananger

1. Go to **Router > Dynamic > BGP**.
2. Set the following information, and select **OK**.

Local As	1
Router ID	10.11.101.110

To set the BGP router information - CLI

```
config router BGP
   set as 1
   set router-id 10.11.101.110
end
```

Add the internal network to the AS

The Company is one AS with the FortiGate unit configured as the BGP border router connecting that AS to the two ISPs ASes. The internal network in the Company's AS must be defined. If there were other networks in the company such as regional offices, they would be added here as well.

To set the networks in the AS - web-based manager

1. Go to **Router > Dynamic > BGP**.
2. In **Networks**, next to **IP/Netmask**, set the following information and select **Add**.

IP/Netmask	10.11.101.0/255.255.255.0

To set the networks in the AS - CLI

```
config router bgp
   config network
   edit 1
      set prefix 10.11.101.0 255.255.255.0
   next
   end
end
```

Add BGP neighbor information

The configuration will not work unless you set **Remote AS** neighbors. This can be done in either the web-based manager or the CLI.

To configure the BGP neighbors - web-based manager

1. Go to **Router > Dynamic > BGP**.
2. Add a **Neighbors IP** of 172.21.111.4 with the **Remote AS** set to 650001, then click **Add/Edit**.
3. Add another **Neighbors IP** of 172.22.222.4 with the **Remote AS** set to 650002, then click **Add/Edit**.

To configure the BGP neighbors - CLI

```
config router BGP
   set as 1
      config neighbor
         edit "172.21.111.4"
            set remote-as 650001
         next
         edit "172.22.222.4"
            set remote-as 650002
         next
      end
   end
```

Additional FortiGate BGP configuration

At this point that is all the settings that can be done in both the web-based manger and the CLI. The remaining configuration must be completed in the CLI.

These additional settings are mainly determined by your ISP requirements. They will determine your timers such as keep alive timers, if extended features like BFD and graceful restart are being used, and so on. For this example, some common simply features are being used to promote faster detections of network failures which will result in better service for the Company's internal network users.

The ISPs do not require authentication between peer routers.

These commands will enable or modify the following features on the FortiGate unit, and where possible on neighboring routers as well:

- `bestpath-med-missing-as-worst` — treats a route without an MED as the worst possible available route due to expected unreliability
- `fast-external-failover` — immediately reset the session information associated with BGP external peers if the link used to reach them goes down
- `graceful-restart*` — advertise reboots to neighbors so they do not see the router as offline, wait before declaring them offline, and how long to wait when they reboot before advertising updates. These commands applies to neighbors and are part of the BGP capabilities. This prevents unneeded routing updates.
- `holdtime-timer` — how long the router will wait for a keepalive message before declaring a router offline. A shorter time will find an offline router faster.
- `keepalive-timer` — how often the router sends out keepalive messages to neighbor routers to maintain those sessions.

- `log-neighbor-changes` — log changes to neighbor routers' status. This can be useful for troubleshooting from both internal and external networks.
- `connect-timer` — how long in seconds the FortiGate unit will try to reach this neighbor before declaring it offline.
- `weight` — used to prefer routes from one neighbor over the other. In this example ISP1 is the primary connection so it is weighted higher than ISP2

To configure additional BGP options - CLI

```
config router bgp
   set bestpath-med-missing-as-worst enable
   set fast-external-failover enable
   set graceful-restart enable
   set graceful-restart-time 120
   set graceful-stalepath-time 180
   set graceful-update-delay 180
   set holdtime-timer 120
   set keepalive-timer 45
   set log-neighbor-changes enable
   config neighbor
      edit 172.21.111.4
         set connect-timer 60
         set description "ISP1"
         set holdtime-timer 120
         set keepalive-timer 45
         set weight 250
      next
      edit 172.22.222.4
         set connect-timer 60
         set description "ISP2"
         set holdtime-timer 120
         set keepalive-timer 45
         set weight 100
      next
   end
end
```

Configuring other networking devices

There are two other networking devices that need to be configured: both ISPs' BGP routers.

The ISPs' routers must add the FortiGate unit as a neighbor so route updates can be sent in both directions. Note that ISP1 is not directly connected to ISP2 that we are aware of.

Inform both of your ISPs of your FortiGate unit's BGP information. Once they have configured their router, you can test your BGP connection to the Internet.

They will require your FortiGate unit's:

- IP address of the connected interface
- The router ID
- Your Company's AS number

Testing this configuration

With the dual-homed BGP configuration in place, you should be able to send and receive traffic, send and receive routes, and not have any routing loops. Testing the networks will confirm things are working as expected.

In general for routing you need to look at the routing table on different routers to see what routes are being installed. You also need to sniff packets to see how traffic is being routed in real time. These two sources of information will normally tell you what you need to know.

Testing of this example's network configuration should be completed in two parts:

- Testing network connectivity
- Verifying the FortiGate unit's routing tables
- Verifying traffic routing
- Verifying the dual-homed side of the configuration

Testing network connectivity

A common first step in testing a new network topology is to test if you can reach the Internet and other locations as you expect you should. If not, you may be prevented be cabling issues, software or other issues.

The easiest way to test connections is to use ping, once you ensure that all the FortiGate unit's interfaces and ISP routers have ping support enabled. Also ensure that the security policies allow ping through the firewall.

Connections to test in this example are the internal network to ISP1's router or the Internet, and the same for ISP2. If you can connect on the external side of the Fortinet unit, try to ping the internal network. Those three tests should prove your basic network connections are working.

Once you have completed testing the network connectivity, turn off ping support on the external interfaces for additional security.

Verifying the FortiGate unit's routing tables

The FortiGate routing table contains the routes stored for future use. If you are expecting certain routes to be there and they are not, that is a good indicator that your configuration is not what you expected.

The CLI command `get router info routing-table details` will provide you with every route's routing protocol, destination address, gateway address, interface, weighting, and if the address is directly connected or not.

If you want to limit the display to BGP routes only, use the CLI command `get router info routing-table bgp`. If there are no BGP routes in the routing table, nothing will be displayed. In the CLI command you can replace BGP with static, or other routing protocols to only display those routes.

If you want to see the contents of the routing information database (RIB), use the CLI command `get router info routing-table database`. This will display the incoming routes that may or may not make it into the routing table.

Verifying traffic routing

Traffic may be reaching the internal network, but it may be using a different route than you think to get there.

Use a browser to try and access the Internet.

If needed, allow traceroute and other diag ports to be opened until things are working properly. Then remove access for them again.

Look for slow hops on the traceroute, or pings to a location, as they may indicate network loops that need to be fixed.

Any locations that have an unresolved traceroute or ping must be examined and fixed.

Use network packet sniffing to ensure traffic is being routed as you expect.

Verifying the dual-homed side of the configuration

Since there are two connections to the Internet in this example, theoretically you can pull the plug on one of the ISP connections, and all traffic will go through the other connection. Alternately, you may choose to remove a default route to one ISP, remove that ISP's neighbor settings, or change the weightings to prefer other other ISP. These alternate ways to test dual-homing do not change physical cabling, which may be preferred in some situations.

If this does not work as expected, things to check include:

- Default static routes — If these are wrong or don't exist, the traffic can't get out.
- BGP neighbor information — If the ISP router information is incorrect, the FortiGate unit won't be able to talk to it.

Redistributing and blocking routes in BGP

During normal BGP operation, peer routers redistribute routes from each other. However, in some specific situations it may be best to not advertise routes from one peer, such as if the peer is redundant with another peer (they share the same routes exactly), if it might be unreliable in some way, or some other reason. The FortiGate can also take routes it learns from other protocols and advertise them in BGP, for example OSPF or RIP. If your Company hosts its own web or email servers, external locations will require routes to your networks to reach those services.

In this example the Company has an internal network in an OSPF area, and is connected to a BGP AS and two BGP peers. Company goes through these two peers to reach the Internet. However, Peer 1 routes will not be advertised to Peer 2. The Company internal user and server networks are running OSPF, and will redistribute those routes to BGP so external locations can reach the web and email servers.

This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate unit
- Testing network configuration

Network layout and assumptions

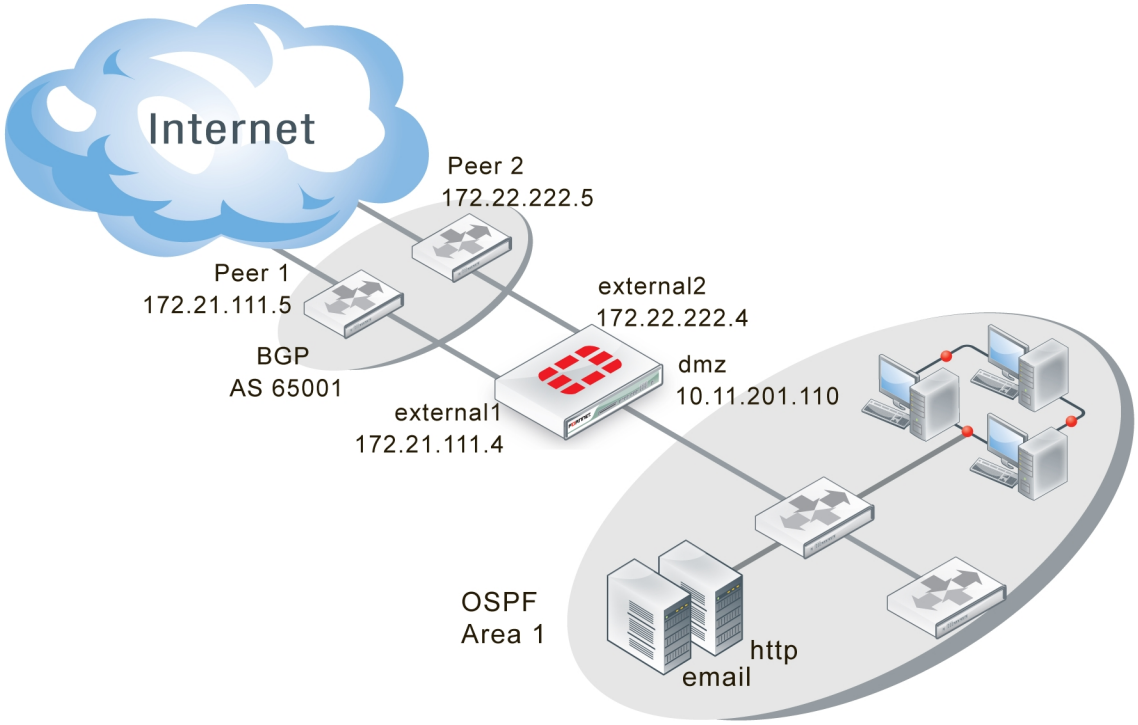
The network layout for the BGP redistributing routes example involves the company network being connected to two BGP peers as shown below. In this configuration the FortiGate unit is the BGP border router between the Company AS, and the peer routers.

The components of the layout include:

- There is only one BGP AS in this example — AS 65001, shared by the FortiGate unit and both peers.
- The Company's FortiGate unit connects to the Internet through two BGP peers.

- The Company internal networks on the dmz interface of the FortiGate unit with an IP of 10.11.201.0/24.
- The FortiGate units' interfaces are connected as follows:
  - port1 (dmz) has IP 10.11.201.110 and is the internal user and server network
  - port2 (external1) has IP 172.21.111.4 and is connected to Peer 1's network
  - port3 (external2) has IP 172.22.222.4 and is connected to Peer 2's network
- Peer 1 has IP 172.21.111.5, and Peer 2 has IP 172.22.222.5.
- OSPF Area 1 is configured on the dmz interface of the FortiGate unit, and is the routing protocol used by the internal users and servers.

BGP network topology



Assumptions

The the BGP redistributing routes configuration procedure follows these assumptions:

- The FortiGate unit has been configured following the Install Guide
- Interfaces port1, port2, and port 3 exist on the FortiGate unit
- We don't know the router manufacturers of Peer 1 and Peer 2
- We don't know what other devices are on the BGP AS or OSPF Area
- All basic configuration can be completed in both GUI and CLI
- Access lists and route maps will only be configured in CLI
- VDOMs are not enabled on the FortiGate unit

Configuring the FortiGate unit

1. Configuring the FortiGate unit — networks and firewalls
2. Configuring the FortiGate unit - BGP
3. Configuring the FortiGate unit - OSPF
4. Configuring other networking devices
5. Configuring ECMP support for BGP

Configuring the FortiGate unit — networks and firewalls

The FortiGate unit has three interfaces connected to networks — two external and one dmz.

Security policies must be in place to allow traffic to flow between these networks.

Firewall services will change depending on which routing protocol is being used on that network — either BGP or OSPF. Beyond that, all services that are allowed will be allowed in both directions due to the internal servers. The services allowed are web-server services (DNS, HTTP, HTTPS, SSH, NTP, FTP*, SYSLOG, and MYSQL), email services (POP3, IMAP, and SMTP), and general troubleshooting services (PING, TRACEROUTE). Those last two can be removed once the network is up and working properly to increase security. Other services can be added later as needed.

To configure the interfaces - GUI

1. Go to **System > Network > Interfaces**.
2. Edit port1 (dmz) interface.
3. Set the following information, and select **OK**.

Alias	dmz
IP/Network Mask	10.11.201.110/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	OSPF internal networks
Administrative Status	Up

4. Edit port2 (external1) interface.
5. Set the following information, and select **OK**.

Alias	external1
IP/Network Mask	172.21.111.4/255.255.255.0
Administrative Access	HTTPS SSH
Description	BGP external Peer 1
Administrative Status	Up

6. Edit port3 (external2) interface.
7. Set the following information, and select **OK**.

Alias	external2
IP/Network Mask	172.22.222.4/255.255.255.0
Administrative Access	HTTPS SSH
Description	BGP external2 Peer2
Administrative Status	Up

To configure the FortiGate interfaces (CLI)

```
config system interface
   edit port1
      set alias dmz
      set ip 10.11.201.110 255.255.255.0
      set allowaccess https ssh ping
      set description "OSPF internal networks"
      set status up
   next
   edit port2
      set alias external1
      set ip 172.21.111.5 255.255.255.0
      set allowaccess https ssh
      set description "external1 Peer 1"
      set status up
   next
   edit port3
      set alias external2
      set ip 172.22.222.5 255.255.255.0
      set allowaccess https ssh
      set description "external2 Peer 2"
      set status up
   next
end
```

To configure the firewall addresses - GUI

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, and set the following information.

Category	Address
Name	BGP_services
Type	Subnet / IP Range
Subnet / IP Range	10.11.201.0 255.255.255.0
Interface	port1

3. Select **OK**.

To configure the firewall addresses - CLI

```
config firewall address
   edit "BGP_services"
      set associated-interface "port1"
      set subnet 10.11.201.0 255.255.255.0
   next
end
```

To configure firewall service groups - GUI

1. Go to **Policy & Objects > Objects > Services.** Under the **Create New** dropdown menu, select **Service Group**.
2. Name the group BGP_Services.
3. Add the following services to the **Members** list: BGP, DNS, FTP, FTP_GET, FTP_PUT, HTTP, HTTPS, IMAP, MYSQL, NTP, PING, POP3, SMTP, SSH, SYSLOG, and TRACEROUTE.
4. Select **OK**.
5. Create another new **Service Group**.
6. Name the group OSPF_Services.
7. Add the following services to the *Members* list: DNS, FTP, FTP_GET, FTP_PUT, HTTP, HTTPS, IMAP, MYSQL, NTP, OSPF, PING, POP3, SMTP, SSH, SYSLOG, and TRACEROUTE.
8. Select **OK**.

To configure firewall service groups - CLI

```
config firewall service group
   edit "BGP_services"
      set member "BGP", "DHCP" "DNS" "FTP" "FTP_GET" "FTP_PUT" "HTTP" "HTTPS" "IMAP"
          "MYSQL" "NTP" "PING" "POP3" "SMTP" "SSH" "TRACEROUTE" "SYSLOG"
   next
   edit "OSPF_services"
      set member "DHCP" "DNS" "FTP" "FTP_GET" "FTP_PUT" "HTTP" "HTTPS" "IMAP" "MYSQL"
          "NTP" "PING" "POP3" "SMTP" "SSH" "TRACEROUTE" "SYSLOG" "OSPF"
   next
end
```

Configuring the FortiGate unit - BGP

The only change from the standard BGP configuration for this example is configuring the blocking Peer 1's routes from being advertised to Peer 2. From the network topology you can guess that both of these peers likely share many routes in common and it makes no sense to advertise unneeded routes.

Blocking Peer 1's routes to Peer 2 is done with distribute-list-out keyword. They allow you to select which routes you will advertise to a neighbor using an access list. In this case we will block all incoming routes from Peer 1 when we send updates to Peer 2. Otherwise Peer 1 and Peer 2 are regular neighbors.

The FortiGate unit will redistribute routes learned from OSPF into BGP.

This is advanced configuration and the commands are only available in the CLI.

To create access list to block Peer 1 - CLI

```
config access-list
   edit "block_peer1"
```

```
      config rule
      edit 1
         set prefix 172.21.111.0 255.255.255.0
         set action deny
         set exact-match enable
      end
   end
end
```

To configure BGP on the FortiGate unit - CLI

```
config router bgp
   set as 65001
      set router-id 10.11.201.110
      config redistribute ospf
         set status enable
      end
      config neighbor
      edit 172.22.222.5
         set remote-as 65001
         set distribute-list-out "block_peer1"
      next
      edit 172.21.111.5
         set remote-as 65001
      end
   end
```

Configuring the FortiGate unit - OSPF

This configuration involves only one OSPF Area, so all traffic will be intra-area. If there were two or more areas with traffic going between them it would be inter-area traffic. These two types are comparable to BGP's traffic within one AS (iBGP) or between multiple ASes (eBPG). Redistributing routes from OSPF to BGP is considered external because either the start or end point is a different routing protocol.

The OSPF configuration is basic apart from redistributing BGP routes learned.

To configure OSPF on the FortiGate unit - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. For Router ID enter `10.11.201.110` and then select **Apply**.
3. Under **Advanced Options** > **Redistribute**, select **BGP** and set the BGP **Metric** to 1.
4. For **Areas**, select **Create New,** enter the following information and then select **OK**.

Area (IP)	`0.0.0.0`
Type	Regular
Authentication	None

5. For **Networks**, select **Create New**.
6. Enter 10.11.201.0/255.255.255.0 for **IP/Netmask**, and select **OK**.
7. For **Interfaces**, select **Create New**.

8. Enter `OSPF_dmz_network` for **Name**.
9. Select `port1(dmz)` for **Interface**, and then select **OK**.

To configure OSPF on the FortiGate unit - CLI

```
config router ospf
   set router-id 10.11.201.110
   config area
      edit 0.0.0.0
         set type regular
         set authentication none
      end
   config network
      edit 1
         set area 0.0.0.0
         set prefix 10.11.201.0 255.255.255.0
      end
   config interface
      edit "OSPF_dmz_network"
         set interface port1(dmz)
         set status enable
      end
   config redistribute bgp
      set status enable
      set metric 1
   end
end
```

Configuring other networking devices

As with all BGP configurations, the peer routers will need to be updated with the FortiGate unit's BGP information including IP address, AS number, and what capabilities are being used such as IPv6, graceful restart, BFD, and so on.

Configuring ECMP support for BGP

"ECMP" stands for "Equal Cost Multiple Path". ECMP is a mechanism that allows multiple routes to the same destination with different next-hops and load-balances routed traffic over those multiple next-hops.

- ECMP only works for routes that are sourced by the same routing protocol (that is: Static Routes, OSPF, or BGP).
- ECMP is enabled by default with 10 paths.
- ECMP with static routes is effective if the routes are configured with the same distance and same priority.

To configure ECMP support - CLI

```
config router bgp
   set ebgp-multipath disable[|enable]
   set ibgp-multipath disable[|enable]
   ...
end
```

Testing network configuration

Testing this configuration involves the standard connectivity checks, but also ensuring that routes are being passed between protocols as expected.

Check the routing table on the FortiGate unit to ensure that routes from both OSPF and BGP are present.

Check the routing table on devices on the OSPF network for routes redistributed from BGP. Also check those devices for connectivity to the Internet.

Check the routing table on Peer 2 to ensure no routes from Peer 1 are present, but routes from the internal OSPF network are present.

For help with troubleshooting, see Redistributing and blocking routes in BGP on page 363.

Open Shortest Path First (OSPF)

This section describes OSPF routing.

The following topics are included in this section:

OSPF Background and concepts
Troubleshooting OSPF
Basic OSPF example
Advanced inter-area OSPF example
Controlling redundant links by cost

OSPF Background and concepts

OSPF (Open Shortest Path First) is a link-state interior routing protocol, that is widely used in large enterprise organizations. It only routes packets within a single autonomous system (AS). This is different from BGP as BGP can communicate between ASes.

This section includes:

- Background
- The parts and terminology of OSPF
- How OSPF works

Background

OSPF version 2 was defined in 1998 in RFC 2328. OSPF was designed to support classless IP addressing, and variable subnet masks. This was a shortcoming of the earlier RIP protocols.

Updates to OSPF version 2 are included in OSPF version 3 defined in 2008 in RFC 5340. OSPF3 includes support for IPv6 addressing where previously OSPF2 only supports IPv4 addressing.

The main benefit of OSPF is that it detects link failures in the network quickly and within seconds has converged network traffic successfully without any networking loops. Also OSPF has many features to control which routes are propagated and which are not, maintaining smaller routing tables. OSPF can also provide better load-balancing on external links than other interior routing protocols.

The parts and terminology of OSPF

Parts and terminology of OSPF includes:

- OSPFv3 and IPv6
- Router ID
- Adjacency
- Designated router (DR) and backup router (BDR)
- Area
- Authentication
- Hello and dead intervals
- Access Lists

OSPFv3 and IPv6

OSPFv3 (OSPF version 3) includes support for IPv6. Generally, all IP addresses are in IPv6 format instead of IPv4. However, OSPFv3 area numbers use the same 32-bit numbering system as OSPFv2, as described in RFC 2740. Likewise, the router ID and area ID are in the same format as OSPFv2.

As with most advanced routing features on your FortiGate unit, IPv6 settings for dynamic routing protocols must be enabled before they will be visible in the GUI. To enable IPv6 configuration in the GUI, enable it in **System > Config > Features**.

For IPv6, the main difference in OSPFv3 is that, rather than using a network statement to enable OSPFv3 on an interface, you define OSPF6 (OSPF for IPv6) interfaces, which are bound to interface and area. This configuration must be done in the CLI, as follows (with sample interfaces and addresses):

```
config router ospf6
   config area
      edit 0.0.0.0
   next
end
config ospf6-interface
   edit "tunnel"
   set interface "to_FGT300A-7"
next
   edit "internal_lan"
   set interface "port1"
next
   set router-id 10.174.0.113
end
```

Note that OSPFv3 neighbors use link-local IPv6 addresses, but with broadcast and point-to-point network types, neighbors are automatically discovered. You only have to manually configure neighbors when using non-broadcast network types.

Router ID

In OSPF, each router has a unique 32-bit number called its Router ID. Often this 32-bit number is written the same as a 32-bit IPv4 address would be written in dotted decimal notation. However some brands of routers, such as Cisco routers, support a router ID entered as an integer instead of an IP address.

It is a good idea to not use IP address in use on the router for the router ID number. The router ID does not have to be a particular IP address on the router. By choosing a different number, it will be harder to get confused which number you are looking at. A good idea can be to use the as much of the area's number as possible. For example if you have 15 routers in area 0.0.0.0 they could be numbered from 0.0.0.1 to 0.0.0.15. If you have an area 1.1.1.1, then routers in that area could start at 1.1.1.10 for example.

You can manually set the router ID on your FortiGate unit.

To manually set an OSPF router ID of 0.0.1.1 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. For **Router ID**, enter `0.0.1.1`.
3. Select **Apply**.

To manually set an OSPF router ID of 0.0.1.1 - CLI

```
config router ospf
   set router-id 0.0.1.1
end
```

Adjacency

In an OSPF routing network, when an OSPF router boots up it sends out OSPF Hello packets to find any neighbors, routers that have access to the same network as the router booting up. Once neighbors are discovered and Hello packets are exchanged, updates are sent, and the Link State databases of both neighbors are synchronized. At this point these neighbors are said to be adjacent.

For two OSPF routers to become neighbors, the following conditions must be met.

- The subnet mask used on both routers must be the same subnet.
- The subnet number derived using the subnet mask and each router's interface IP address must match.
- The Hello interval & The Dead interval must match.
- The routers must have the same OSPF area ID. If they are in different areas, they are not neighbors.
- If authentication is used, they must pass authentication checks.

If any of these parameters are different between the two routers, the routers do not become OSPF neighbors and cannot be adjacent. If the routers become neighbors, they are adjacent.

Adjacency and neighbors

Neighbor routers can be in a Two-Way state, and not be adjacent. Adjacent routers normally have a neighbor state of FULL. Neighbors only exchange Hello packets, and do not exchange routing updates. Adjacent routers exchange LSAs (LSDB information) as well as Hello packets. A good example of an adjacent pair of routers is the DR and BDR.

You can check on the state of an OSPF neighbor using the CLI command `get router info ospf neighbor all`. See OSPF Background and concepts on page 371.

Why adjacency is important

It is important to have adjacent pairs of routers in the OSPF routing domain because routing protocol packets are only passed between adjacent routers. This means adjacency is required for two OSPF routers to exchange routes.

If there is no adjacency between two routers, such as one on the 172.20.120.0 network and another on the 10.11.101.0 network, the routers do not exchange routes. This makes sense because if all OSPF routers on the OSPF domain exchanged updates it would flood the network.

Also, it is better for updates to progress through adjacent routers to ensure there are no outages along the way. Otherwise, updates could skip over routers that are potentially offline, causing longer routing outages and delays while the OSPF domain learns of this outage later on.

If the OSPF network has multiple border routers and multiple connections to external networks, the designated router (DR) determines which router pairs become adjacent. The DR can accomplish this because it maintains the complete topology of the OSPF domain, including which router pairs are adjacent.

The BDR also has this information in case the DR goes offline.

Designated router (DR) and backup router (BDR)

In OSPF a router can have a number of different roles to play.

A designated router (DR) is the designated broadcasting router interface for an AS. It looks after all the initial contact and other routing administration traffic. Having only one router do all this greatly reduces the network traffic and collisions.

If something happens and the designated router goes offline, the backup designated router (BDR) takes over. An OSPF FortiGate unit interface can become either a DR or BDR. Both the DR and the BDR cover the same area, and are elected at the same time. The election process doesn't have many rules, but the exceptions can become complex.

Benefits

The OSPF concept of the designated router is a big step above RIP. With all RIP routers doing their own updates all the time, RIP suffers from frequent and sometimes unnecessary updates that can slow down your network. With OSPF, not only do routing changes only happen when a link-state changes instead of any tiny change to the routing table, but the designated router reduces this overhead traffic even more.

However, smaller network topologies may only have a couple routers besides the designated router. This may seem excessive, but it maintains the proper OSPF form and it will still reduce the administration traffic but to a lesser extent than on a large network. Also, your network topology will be ready whenever you choose to expand your network.

DR and BDR election

An election chooses the DR and BDR from all the available routers. The election is primarily based on the priority setting of the routers—the highest priority becomes the DR, and the second highest becomes BDR. To resolve any ties, the router with the highest router ID wins. For example 192.168.0.1 would win over 10.1.1.2.

The router priority can vary from 0 to 255, but at 0 a router will never become a DR or BDR. If a router with a higher priority comes on line after the election, it must wait until after the DR and BDR go offline before it would become the DR.

If the original DR goes offline, but then is available when the BDR goes offline later on, the original DR will be promoted back to DR without an election leaving the new BDR as it is.

With your FortiGate unit, to configure the port1 interface to be a potential OSPF designated router or backup designed router called `ospf_DR` on the network, you need to raise the priority of the router to a very high number such as 250 out of 255. This will ensure the router has a chance to be a DR, but will not guarantee that it will be one. Give the FortiGate a high router ID—such as 192.168.1.1 instead of 10.1.1.1—to help ensure it becomes a DR, but that is not part of this example. Enter the following command:

```
config router ospf
   config ospf-interface
   edit "ospf_DR"
      set priority 250
   end
end
```

Area

An OSPF area is a smaller part of the larger OSPF AS. Areas are used to limit the link-state updates that are sent out. The flooding used for these updates would overwhelm a large network, so it is divided into these smaller areas for manageability.

Within an area if there are two or more routers that are viable, there will always be a designated router (DR) and a backup DR (BDR). For more on these router roles, see Designated router (DR) and backup router (BDR) on page 374.

Defining a private OSPF area, involves:

- Assigning a 32-bit number to the area that is unique on your network
- Defining the characteristics of one or more OSPF areas
- Creating associations between the OSPF areas that you defined and the local networks to include in the OSPF area
- If required, adjusting the settings of OSPF-enabled interfaces.

IPv6 OSPF area numbers use the same 32-bit number notation as IPv4 OSPF.

If you are using the web-based manager to perform these tasks, follow the procedures summarized below.

FortiGate units support the four main types of OSPF area:

- Backbone area
- Stub area
- NSSA
- Regular area

Backbone area

Every OSPF network has at least one AS, and every OSPF network has a backbone area. The backbone is the main area, or possibly the only area. All other OSPF areas are connected to a backbone area. This means if two areas want to pass routing information back and forth, that routing information will go through the backbone on its way between those areas. For this reason the backbone not only has to connect to all other areas in the network, but also be uninterrupted to be able to pass traffic to all points of the network.

The backbone area is referred to as area 0 because it has an IP address of 0.0.0.0.

Stub area

A stub area is an OSPF area that receives no outside routes advertised into it, and all routing in it is based on a default route. This essentially isolates it from outside areas.

Stub areas are useful for small networks that are part of a larger organization, especially if the networking equipment can't handle routing large amounts of traffic passing through, or there are other reasons to prevent outside traffic, such as security. For example most organizations don't want their accounting department to be the center of their network with everyone's traffic passing through there. It would increase the security risks, slow down their network, and it generally doesn't make sense.

A variation on the stub area is the totally stubby area. It is a stub area that does not allow summarized routes.

NSSA

A not-so-stubby-area (NSSA) is a stub area that allows for external routes to be injected into it. While it still does not allow routes from external areas, it is not limited to only using he default route for internal routing.

Regular area

A regular area is what all the other ASes are, all the non-backbone, non-stub, non-NSSA areas. A regular area generally has a connection to the backbone, does receive advertisements of outside routes, and does not have an area number of 0.0.0.0.

Authentication

In the OSPF packet header are two authentication related fields —AuType, and Authentication.

All OSPF packet traffic is authenticated. Multiple types of authentication are supported in OSPFv2. However in OSPFv3, there is no authentication built-in but it is assumed that IPsec will be used for authentication instead.

Packets that fail authentication are discarded.

Null authentication

Null authentication indicates there is no authentication being used. In this case the 16-byte Authentication field is not checked, and can be any value. However checksumming is still used to locate errors. On your FortiGate this is the `none` option for authentication.

Simple Password authentication

Simple password refers to a standard plain text string of characters. The same password is used for all transactions on a network. The main use of this type of authentication is to prevent routers from accidently joining the network. Simple password authentication is vulnerable to many forms of attack, and is not recommended as a secure form of authentication.

Cryptographic authentication

Cryptographic authentication involves the use of a shared secret key to authenticate all router traffic on a network. The key is never sent over the network in the clear—a packet is sent and a condensed and encrypted form of the packet is appended to the end of the packet. A non-repeating sequence number is included in the OSPF packet to protect against replay attacks that could try to use already sent packets to disrupt the network. When a packet is accepted as authentic the authentication sequence number is set to the packet sequence number. If a replay attack is attempted, the packet sent will be out of sequence and ignored.

Your FortiGate unit supports all three levels of authentication through the authentication keyword associated with creating an OSPF interface .

For example to create an OSPF interface called `Accounting` on the port1 interface that is a broadcast interface, has a hello interval of 10 seconds, has a dead interval of 40 seconds, uses text authentication (simple password) with a password of “ospf_test”, enter the command:

```
config router ospf
   config ospf-interface
   edit Accounting
      set interface port1
      set network-type broadcast
```

```
      set hello-interval 10
      set dead-interval 40
      set authentication text
      set authentication-key "ospf_test"
   end
end
```

Hello and dead intervals

The OSPF Hello protocol is used to discover and maintain communications with neighboring routers.

Hello packets are sent out at a regular interval for this purpose. The DR sends out the Hello packets. In a broadcast network, the multicast address of 224.0.0.5 is used to send out Hello packets. New routers on the network listen for and reply to these packets to join the OSPF area. If a new router never receives a Hello packet, other routers will not know it is there and will not communicate with it. However, once a new router is discovered the DR adds it to the list of routers in that area and it is integrated into the routing calculations.

Dead interval is the time other routers will wait before declaring a neighbor dead (offline). Setting a reasonable dead interval is very important. If this interval is too short, routers will be declared offline when they are just slow or momentarily inaccessible, and link-state updates will happen more than they need to, using more bandwidth. If the dead interval is too long, it will slow down network traffic overall if online routers attempt to contact offline ones instead of re-routing traffic.

FortiOS also supports OSPF fast-hello, which provides a way of sending multiple Hello packets per second. This is achieved by setting a dead-interval to one second. The hello-multiplier, which can be any number between 4 and 10, determines the number of Hello packets that will be sent every second. The CLI syntax for OSPF fast-hello follows:

```
config ospf-interface
   edit ospf1
      set interface port1
      set network-type broadcast
      set dead-interval 1
      set hello-multiplier 4
end
```

Access Lists

Access lists are filters used by FortiGate unit OSPF routing. An access list provides a list of IP addresses and the action to take for them — essentially an access list makes it easy to group addresses that will be treated the same into the same group, independent of their subnets or other matching qualities. You add a rule for each address or subnet that you want to include, specifying the action to take for it. For example if you wanted all traffic from one department to be routed a particular way, even in different buildings, you can add all the addresses to an access list and then handle that list all at once.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

Access lists greatly speed up configuration and network management. When there is a problem, you can check each list instead of individual addresses. Also, it eases troubleshooting since if all addresses on one list have problems, it eliminates many possible causes right away.

If you are using the OSPF+ IPv6 protocols you will need to use access-list6, the IPv6 version of access list. The only difference is that access-list6 uses IPv6 addresses.

For example, if you want to create an access list called `test_list` that only allows an exact match of `10.10.10.10` and `11.11.11.11`, enter the command:

```
config router access-list
   edit test_list
   config rule
      edit 1
         set prefix 10.10.10.10 255.255.255.255
         set action allow
         set exact-match enable
      next
      edit 2
         set prefix 11.11.11.11 255.255.255.255
         set action allow
         set exact-match enable
      end
   end
```

Another example is if you want to deny ranges of addresses in IPv6 that start with the IPv6 equivalents of 10.10.10.10 and 11.11.11.11, enter the command access-list6 as follows:

```
config router access-list6
   edit test_list_ip6
      config rule
         edit 1
            set prefix6 2002:A0A:A0A:0:0:0:0:0:/48
            set action deny
         next
         edit 2
            set prefix6 2002:B0B:B0B:0:0:0:0:0/48
            set action deny
         end
```

To use an access_list, you must call it from a routing protocol such as RIP. The following example uses the access_list from the earlier example called test_list to match routes coming in on the port1 interface. When there is a match, it will add 3 to the hop count metric for those routes to artificially decrease their priority. Enter the following command:

```
config router ospf
   config distribute-list
      edit 5
         set access-list test_list
         set protocol connected
      end
```

If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose.

How OSPF works

An OSPF installation consists of one or more areas. An OSPF area is typically divided into logical areas linked by Area Border Routers. A group of contiguous networks form an area. An Area Border Router (ABR) links one or more areas to the OSPF network backbone (area ID 0). See Dynamic Routing Overview on page 279.

OSPF is an interior routing protocol. It includes a backbone AS, and possibly additional ASes. The DR and BDR are elected from potential routers with the highest priorities. The DR handles much of the administration to lower the network traffic required. New routers are discovered through hello packets sent from the DR using the multicast address of 224.0.0.5. If the DR goes offline at any time, the BDR has a complete table of routes that is uses when it takes over as the DR router.

OSPF does not use UDP or TCP, but is encapsulated directly in IP datagrams as protocol 89. This is in contrast to RIP, or BGP. OSPF handles its own error detection and correction functions.

The OSPF protocol, when running on IPv4, can operate securely between routers, optionally using a variety of authentication methods to allow only trusted routers to participate in routing. OSPFv3, running on IPv6, no longer supports protocol-internal authentication. Instead, it relies on IPv6 protocol security (IPsec).

Other important parts of how OSPF works includes:

- OSPF router discovery
- How OSPF works on FortiGate units
- External routes
- Link-state Database (LSDB) and route updates
- OSPF packets

OSPF router discovery

OSPF-enabled routers generate Link-State Advertisements (LSA) and send them to their neighbors whenever the status of a neighbor changes or a new neighbor comes online. As long as the OSPF network is stable, LSAs between OSPF neighbors do not occur. An LSA identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination. All LSA exchanges between OSPF-enabled routers are authenticated.

When a network of OSPF routers comes online, the follow steps occur.

1. When OSPF routers come online, they send out Hello packets to find other OSPF routers on their network segment.
2. When they discover other routers on their network segment, generally they become adjacent. Adjacent routers can exchange routing updates. See Adjacency on page 373.
3. A DR and BDR are elected from the available routers using priority settings, and router ID. See Designated router (DR) and backup router (BDR) on page 374, and OSPF Background and concepts on page 371.
4. Link state updates are sent between adjacent routers to map the topology of the OSPF area.
5. Once complete, the DR floods the network with the updates to ensure all OSPF routers in the area have the same OSPF route database. After the initial update, there are very few required updates if the network is stable.

How OSPF works on FortiGate units

When a FortiGate unit interface is connected to an OSPF area, that unit can participate in OSPF communications. FortiGate units use the OSPF Hello protocol to acquire neighbors in an area. A neighbor is any router that is directly connected to the same area as the FortiGate unit, and ideally is adjacent with a state of Full. After initial contact, the FortiGate unit exchanges Hello packets with its OSPF neighbors regularly to confirm that the neighbors can be reached.

The number of routes that a FortiGate unit can learn through OSPF depends on the network topology. A single unit can support tens of thousands of routes if the OSPF network is configured properly.

External routes

OSPF is an internal routing protocol. OSPF external routes are routes where the destination using a routing protocol other than OSPF. OSPF handles external routes by adjusting the cost of the route to include the cost of the other routing protocol. There are two methods of calculating this cost, used for OSPF E1 and OSPF E2.

OSPF external1 (E1)

In OSPF E1 the destination is outside of the OSPF domain. This requires a different metric to be used beyond the normal OSPF metrics. The new metric of a redistributed route is calculated by adding the external cost and the OSPF cost together.

OSPF external2 (E2)

OSPF E2 is the default external type when routes are redistributed outside of OSPF. With OSPF E2, the metric of the redistributed route is equivalent to the external cost only, expressed as an OSPF cost. Dropping the OSPF portion can be useful in a number of situations, on border routers that have no OSPF portion for example or where the OSPF routing cost is negligible compared to the external routing cost.

Comparing E1 and E2

The best way to understand OSPF E1 and E2 routes is to check routing tables on OSPF routers. If you look at the routes on an OSPF border router, the redistributed routes will have an associated cost that represents only the external route, as there is no OSPF cost to the route due to it already being on the edge of the OSPF domain. However, if you look at that same route on a different OSPF router inside the OSPF routing domain, it will have a higher associated cost - essentially the external cost plus the cost over the OSPF domain to that border router. The border router uses OSPF E2, where the internal OSPF router uses OSPF E1 for the same route.

Viewing external routes

When you are trying to determine the costs for routes in your network to predict how traffic will be routed, you need to see the external OSPF routes and their associated costs. On your FortiGate unit, you find this information through your CLI.

To view external routes - CLI

You can view the whole routing table using `get router info routing-table all` to see all the routes including the OSPF external routes, or for a shorter list you can use the command `get router info routing-table ospf`. The letter at the left will be either E1 or E2 for external OSPF routes. The output of will look similar to the following, depending on what routes are in your routing table.

```
FGT620B# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

O*E2   0.0.0.0/0 [110/10] via 10.1.1.3, tunnel_wan2, 00:02:11
O      10.0.0.1/32 [110/300] via 10.1.1.3, tunnel_wan2, 00:02:11
S      0.0.0.0/0 [10/0] via 192.168.183.254, port2
S      1.0.0.0/8 [10/0] via 192.168.183.254, port2
```

Link-state Database (LSDB) and route updates

OSPF is based on links. The links between adjacent neighbor routers allow updates to be passed along the network. Network links allow the DR to flood the area with Link-state database (LSDB) updates. External links allow the OSPF area to connect to destinations outside the OSPF autonomous system. Information about these links is passed throughout the OSPF network as link-state updates.

The LSDB contains the information that defines the complete OSPF area, but the LSDB is not the routing table. It contains the information from all the link-state updates passed along the network. When there are no more changes required, and the network is stable then the LSDB on each router in the network will be the same. The DR will flood the LSDB to the area to ensure each router has the same LSDB.

To calculate the best route (shortest path) to a destination, the FortiGate unit applies the Shortest Path First (SPF) algorithm, based on Dijkstra's algorithm, to the accumulated link-state information. OSPF uses relative path cost metric for choosing the best route. The path cost can be any metric, but is typically the bandwidth of the path, how fast traffic will get from one point to another.

The path cost, similar to "distance" for RIP, imposes a penalty on the outgoing direction of a FortiGate unit interface. The path cost of a route is calculated by adding together all of the costs associated with the outgoing interfaces along the path to the destination. The lowest overall path cost indicates the best route, and generally the fastest route. Some brands of OSPF routers, such as Cisco, implement cost as a direct result of bandwidth between the routers. Generally this is a good cost metric because larger bandwidth means more traffic can travel without slowing down. To achieve this type of cost metric on FortiGate units, you need to set the cost for each interface manually in the CLI.

The inter-area routes may not be calculated when a Cisco type ABR has no fully adjacent neighbor in the backbone area. In this situation, the router considers summary-LSAs from all Actively summary-LSAs from all Actively Attached areas (RFC 3509).

The FortiGate unit dynamically updates its routing table based on the results of the SPF calculation to ensure that an OSPF packet will be routed using the shortest path to its destination. Depending on the network topology, the entries in the FortiGate unit routing table may include:

- The addresses of networks in the local OSPF area (to which packets are sent directly)
- Routes to OSPF area border routers (to which packets destined for another area are sent)
- If the network contains OSPF areas and non-OSPF domains, routes to area boundary routers, which reside on the OSPF network backbone and are configured to forward packets to destinations outside the OSPF AS.

OSPF Route updates

Once the OSPF domain is established, there should be few updates required on a stable network. When updates occur and a decision is required concerning a new route, this is the general procedure.

Our router gets a new route, and needs to decide if it should go in the routing table.

The router has an up to date LSDB of the entire area, containing information about each router, the next hop to it, and most importantly the cost to get there.

Our router, turns the LSDB into a shortest path first (SPF) tree using Dijkstra's algorithm. It doesn't matter if there is more than one path to a router on the network, the SPF tree only cares about the shortest path to that router.

Once the SPF tree has been created, and shows the shortest paths to all the OSPF routers on the network, the work is done. If the new route is the best route, it will be part of that tree. If it is not the shortest route, it will not be included in the LSDB.

If there has been a change from the initial LSDB to the new SPF tree, a link state update will be sent out to let the other routers know about the change so they can update their LSDBs as well. This is vital since all routers on the OSPF area must have the same LSDB.

If there was no change between the LSDB and the SPF tree, no action is taken.

OSPF packets

Every OSPF packet starts with a standard 24-byte header, and another 24 bytes of information or more. The header contains all the information necessary to determine whether the packet should be accepted for further processing.

OSPF packet

1-byte Version field	1-byte Type field	2-byte Packet length	3-byte Router ID
4-byte Area ID	2-byte Checksum	2-byte Auth Type	8-byte Authentication
4-byte Network Mask	2-byte Hello interval	1-byte Options field	1-byte Router Priority
4-byte Dead Router interval	4-byte DR field	4-byte BDR field	4-byte Neighbor ID

The following descriptions summarize the OSPF packet header fields.

Version field — The OSPF version number. This specification documents version 2 of the protocol.

Type field — There are 5 OSPF packet types. From one to five, respectively, they are Hello, Database Description, Link State Request, Link State Update, and Link State Acknowledgment.

Packet length — The length of the OSPF protocol packet in bytes. This length includes the standard OSPF 24-byte header, so all OSPF packets are at 24-bytes long.

Router ID — The Router ID of the packet's source.

Area ID — A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Most travel a single hop only. Packets travelling over a virtual link are labelled with the backbone Area ID of 0.0.0.0.

Checksum — The standard IP checksum of the entire contents of the packet, starting with the OSPF packet header but excluding the 64-bit authentication field. This checksum is calculated as the 16-bit one's complement of the one's complement sum of all the 16-bit words in the packet, excepting the authentication field. If the packet's length is not an integral number of 16-bit words, the packet is padded with a byte of zero before checksumming. The checksum is considered to be part of the packet authentication procedure; for some authentication types the checksum calculation is omitted.

Auth Type — Identifies the authentication procedure to be used for the packet. Authentication types include Null authentication (0), Simple password (1), Cryptographic authentication (2), and all others are reserved for future use.

Authentication — A 64-bit field for use by the authentication scheme. When AuType indicates no authentication is being used, the Authentication fields is not checked and can be any value. When AuType is set to 2 (Cryptographic authentication), the 64-bit authentication field is split into the following four fields: Zero field, Key ID field, Authentication data length field, and Cryptographic sequence field.

The Key ID field indicates the key and algorithm used to create the message digest appended to the packet. The authentication data length field indicates how many bytes long the message digest is, and the cryptographic sequence number is at non-decreasing number that is set when the packet is received and authenticated to prevent replay attacks.

Network Mask — The subnet where this packet is valid.

Hello interval — The period of time between sending out Hello packets. See Hello and dead intervals on page 377.

Options field — The OSPF protocol defines several optional capabilities. A router indicates the optional capabilities that it supports in its OSPF Hello packets, Database Description packets and in its LSAs. This enables routers supporting a mix of optional capabilities to coexist in a single Autonomous System.

Router priority — The priority between 0 and 255 that determines which routers become the DR and BDR. See Designated router (DR) and backup router (BDR) on page 374.

Dead router interval — The period of time when there is no response from a router before it is declared dead. See Hello and dead intervals on page 377.

DR and BDR fields — The DR and BDR fields each list the router that fills that role on this network, generally the routers with the highest priorities. See Designated router (DR) and backup router (BDR) on page 374.

Neighbor ID — The ID number of a neighboring router. This ID is used to discover new routers and respond to them.

Troubleshooting OSPF

As with other dynamic routing protocols, OSPF has some issues that may need troubleshooting from time to time. For basic troubleshooting, see the FortiOS Handbook Troubleshooting chapter.

The more common issues include:

- Clearing OSPF routes from the routing table
- Checking the state of OSPF neighbors
- Passive interface problems
- Timer problems
- Bi-directional Forwarding Detection (BFD)
- Authentication issues
- DR and BDR election issues

Clearing OSPF routes from the routing table

If you think the wrong route has been added to your routing table and you want to check it out, you first have to remove that route from your table before seeing if it is added back in or not. You can clear all or some OSPF neighbor connections (sessions) using the `execute router clear ospf` command. The exec router clear command is much more limiting for OSPF than it is for BGP. See Border Gateway Protocol (BGP) on page 332.

For example, if you have routes in the OSPF routing table and you want to clear the specific route to IP address 10.10.10.1, you will have to clear all the OSPF entries. Enter the command:

```
execute router clear ospf process
```

Checking the state of OSPF neighbors

In OSPF each router sends out link state advertisements to find other routers on its network segment, and to create adjacencies with some of those routers. This is important because routing updates are only passed between adjacent routers. If two routers you believe to be adjacent are not, that can be the source of routing failures.

To identify this problem, you need to check the state of the OSPF neighbors of your FortiGate unit. Use the CLI command `get router info ospf neighbor all` to see all the neighbors for your FortiGate unit. You will see output in the form of:

```
FGT1 # get router info ospf neighbor
OSPF process 0:
Neighbor ID  Pri  State    Dead Time Address Interface
10.0.0.2     1    Full/ -  00:00:39 10.1.1.2 tunnel_wan1
10.0.0.2     1    Full/ -  00:00:34 10.1.1.4 tunnel_wan2
```

The important information here is the `State` column. Any neighbors that are not adjacent to your FortiGate unit will be reported in this column as something other than `Full`. If the state is `Down`, that router is offline.

Passive interface problems

A passive OSPF interface doesn't send out any updates. This means it can't be a DR, BDR, or an area border router among other things. It will depend on other neighbor routers to update its link-state table.

Passive interfaces can cause problems when they aren't receiving the routing updates you expect from their neighbors. This will result in the passive OSPF FortiGate unit interface having an incomplete or out-of-date link-state database, and it will not be able to properly route its traffic. It is possible that the passive interface is causing a hole in the network where no routers are passing updates to each other, however this is a rare situation.

If a passive interface is causing problems, there are simple methods to determine it is the cause. The easiest method is to make it an active interface, and if the issues disappear, then that was the cause. Another method is to examine the OSPF routing table and related information to see if it is incomplete compared to other neighbor routers. If this is the case, you can clear the routing table, reset the device and allow it to repopulate the table.

If you cannot make the interface active for some reason, you will have to change your network to fix the "hole" by adding more routers, or changing the relationship between the passive router's neighbors to provide better coverage.

Timer problems

A timer mismatch is when two routers have different values set for the same timer. For example if one router declares a router dead after 45 seconds and another waits for 4 minutes that difference in time will result in those two routers being out of synch for that period of time—one will still see that offline router as being online.

The easiest method to check the timers is to check the configuration on each router. Another method is to sniff some packets, and read the timer values in the packets themselves from different routers. Each packet contains the hello interval, and dead interval periods, so you can compare them easily enough.

Bi-directional Forwarding Detection (BFD)

Bi-directional Forwarding Detection (BFD) is a protocol used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated.

Authentication issues

OSPF has a number of authentication methods you can choose from. You may encounter problems with routers not authenticating as you expect. This will likely appear simply as one or more routers that have a blind spot in their routing - they won't acknowledge a router. This can be a problem if that router connects areas to the backbone as it will appear to be offline and unusable.

To confirm this is the issue, the easiest method is to turn off authentication on the neighboring routers. With no authentication between any routers, everything should flow normally.

Another method to confirm that authentication is the problem is to sniff packets, and look at their contents. The authentication type and password are right in the packets which makes it easy to confirm they are what you expect during real time. Its possible one or more routers is not configured as you expect and may be using the wrong authentication. This method is especially useful if there are a group of routers with these problems—it may only be one router causing the problem that is seen in multiple routers.

Once you have confirmed the problem is authentication related, you can decide how to handle it. You can turn off authentication and take your time to determine how to get your preferred authentication type back online. You can try another type of authentication, such as text instead of md5, which may have more success and still provide some level of protection. The important part is that once you confirm the problem, you can decide how to fix it properly.

DR and BDR election issues

You can force a particular router to become the DR and BDR by setting their priorities higher than any other OSPF routers in the area. This is a good idea when those routers have more resources to handle the traffic and extra work of the DR and BDR roles, since not all routers may be able to handle all that traffic.

However, if you set all the other routers to not have a chance at being elected, a priority of zero, you can run into problems if the DR and BDR go offline. The good part is that you will have some warning generally as the DR goes offline and the BDR is promoted to the DR position. But if the network segment with both the DR and BDR goes down, your network will have no way to send hello packets, send updates, or the other tasks the DR performs.

The solution to this is to always allow routers to have a chance at being promoted, even if you set their priority to one. In that case they would be the last choice, but if there are no other candidates you want that router to become the DR. Most networks would have already alerted you to the equipment problems, so this would be a temporary measure to keep the network traffic moving until you can find and fix the problem to get the real DR back online.

Basic OSPF example

This example sets up an OSPF network at a small office. There are 3 routers, all running OSPF v2. The border router connects to a BGP network.

All three routers in this example are FortiGate units. Router1 will be the designated router (DR) and router2 will be the backup DR (BDR) due to their priorities. Router3 will not be considered for either the DR or BDR elections.

Instead, Router3 is the area border router (ASBR) routing all traffic to the ISP's BGP router on its way to the Internet.

Router2 has a modem connected that provides dialup access to the Internet as well, at a reduced bandwidth. This is a PPPoE connection to a DSL modem. This provides an alternate route to the Internet if the other route goes down. The DSL connection is slow, and is charged by the amount of traffic. For these reasons OSPF will highly favor Router3's Internet access.

The DSL connection connects to an OSPF network with the ISP, so no redistribution of routes is required. The ISP network does have to be added to that router's configuration however.

This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate units
- Configuring OSPF on the FortiGate units
- Configuring other networking devices
- Testing network configuration

Network layout and assumptions

There are three FortiGate units acting as OSPF v2 routers on the network—Router1, Router2, and Router3. Router1 will be the designated router (DR), and Router 2 the BDR. Router3 is the area border router (ASBR) that connects to the external ISP router running BGP. Router2 has a PPPoE DSL connection that can access the Internet.

The Head Office network is connected to Router1 and Router2 on the 10.11.101.0 subnet.

Router1 and Router3 are connected over the 10.11.103.0 subnet.

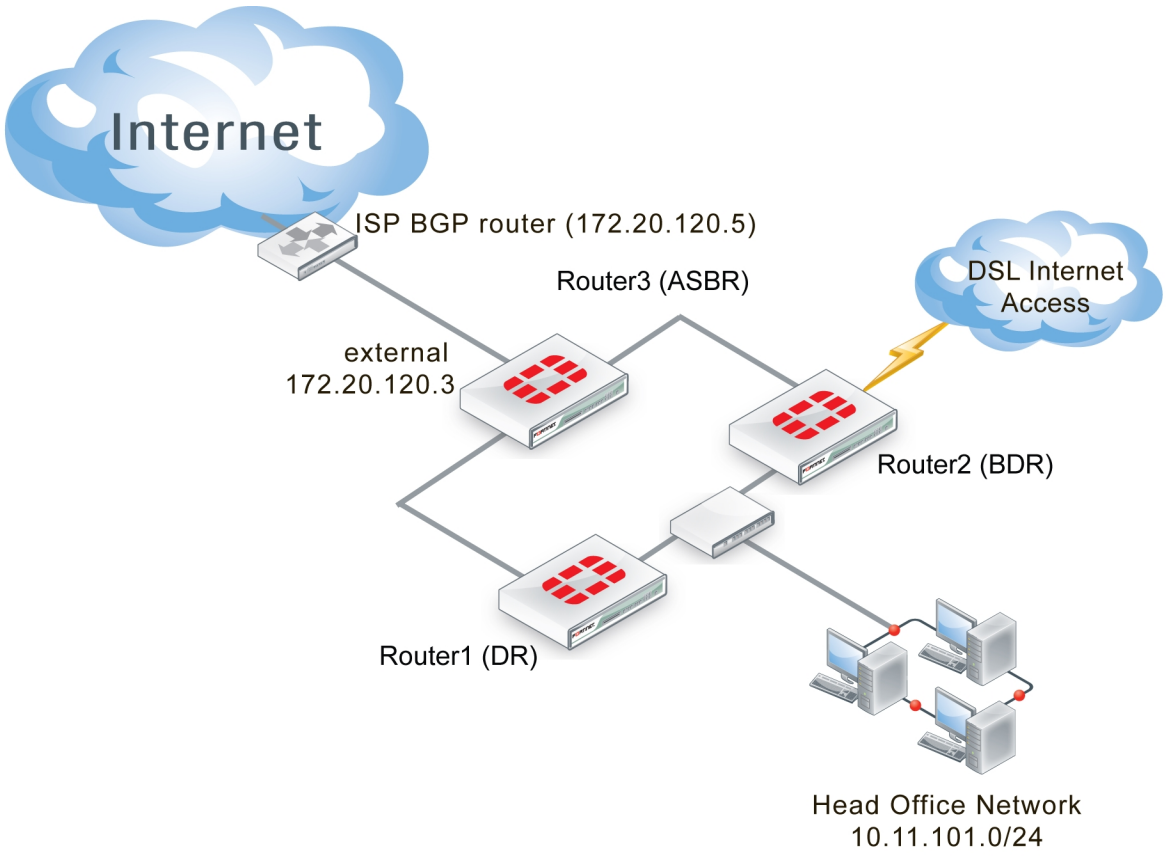
Router2 and Router3 are connected over the 10.11.102.0 subnet.

The following table lists the router, interface, address, and role it is assigned.

Routers, interfaces, and IP addresses for basic OSPF example network

Router name	Interface	IP address	Interface is connected to:
Router1 (DR)	Internal (port1)	10.11.101.1	Head office network, and Router2
	External (port2)	10.11.102.1	Router3
Router2 (BDR)	Internal (port1)	10.11.101.2	Head office network, and Router1
	External (port2)	10.11.103.2	Router3
	DSL (port3)	10.12.101.2	PPPoE DSL access
	Internal1 (port1)	10.11.102.3	Router1
Router3 (ASBR)	Internal2 (port2)	10.11.103.3	Router2
	External (port3)	172.20.120.3	ISP's BGP network

Basic OSPF network topology



Note that other subnets can be added to the internal interfaces without changing the configuration.

Assumptions

- The FortiGate units used in this example have interfaces named port1, port2, and port3.
- All FortiGate units in this example have factory default configuration with FortiOS 5.2 firmware installed, and are in NAT/Route operation mode.
- Basic firewalls are in place to allow unfiltered traffic between all connected interfaces in both directions.
- This OSPF network is not connected to any other OSPF networks.
- Both Internet connections are always available.
- The modem connection is very slow and expensive.
- Other devices may be on the network, but do not affect this basic configuration.
- Router3 is responsible for redistributing all routes into and out of the OSPF AS.

Configuring the FortiGate units

Each FortiGate unit needs the interfaces, and basic system information such as hostname configured.

This section includes:

- Configuring Router1
- Configuring Router2

- Configuring Router3

Configuring Router1

Router1 has two interfaces connected to the network—internal (port1) and external (port2). Its host name must be changed to Router1.

To configure Router1 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Beside the host name, select **Change**.
3. Enter a hostname of `Router1`, and select **OK**.
4. Go to **System > Network > Interfaces**, edit port1, set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.1/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Head office and Router2
Administrative Status	Up

5. Edit port2, set the following information, and select **OK**.

Alias	External
IP/Network Mask	10.11.102.1/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router3
Administrative Status	Up

Configuring Router2

Router2 configuration is the same as Router1, except Router2 also has the DSL interface to configure.

The DSL interface is configured with a username of “user1” and a password of “ospf_example”. The default gateway will be retrieved from the ISP, and the defaults will be used for the rest of the PPPoE settings.

To configure Router2 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Beside the host name, select **Change**.
3. Enter a hostname of `Router2`, and select **OK**.
4. Go to **System > Network > Interfaces**, edit port1, set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.2/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Head office and Router1
Administrative Status	Up

5. Edit port2, set the following information, and select **OK**.

Alias	External
IP/Network Mask	10.11.103.2/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router3
Administrative Status	Up

6. Edit DSL (port3), set the following information, and select **OK**.

Alias	DSL
Addressing Mode	PPPoE
Username	user1
Password	ospf_example
Unnumbered IP	10.12.101.2/255.255.255.0
Retrieve default gateway from server	Enable
Administrative Access	HTTPS SSH PING
Description	DSL
Administrative Status	Up

Configuring Router3

Router3 is similar to Router1 and Router2 configurations. The main difference is the External (port3) interface connected to the ISP BGP network which has no administration access enabled for security reasons.

To configure Router3 interfaces - web-based manager

1. Go to **System > Status > Dashboard**.
2. Next to hostname, select **Change**.
3. Enter a hostname of `Router3`, and select **OK**.
4. Go to **System > Network > Interfaces, e**dit port1, set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.102.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router1
Administrative Status	Up

5. Edit port2, set the following information, and select **OK**.

Alias	Internal2
IP/Network Mask	10.11.103.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router2
Administrative Status	Up

6. Edit port3, set the following information, and select **OK**.

Alias	External
IP/Network Mask	172.20.120.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	ISP BGP
Administrative Status	Up

Configuring OSPF on the FortiGate units

With the interfaces configured, now the FortiGate units can be configured for OSPF on those interfaces. All routers are part of the backbone 0.0.0.0 area, so there is no inter-area communications needed.

For a simple configuration there will be no authentication, no graceful restart or other advanced features, and timers will be left at their defaults. Also the costs for all interfaces will be left at 10, except for the modem and ISP interfaces where cost will be used to load balance traffic. Nearly all advanced features of OSPF are only available from the CLI.

The network that is defined covers all the subnets used in this example - 10.11.101.0, 10.11.102.0, and 10.11.103.0. All routes for these subnets will be advertised. If there are other interfaces on the FortiGate units that you do not want included in the OSPF routes, ensure those interfaces use a different subnet outside of the 10.11.0.0 network. If you want all interfaces to be advertised you can use an OSPF network of 0.0.0.0 .

Each router will configure:

- Router ID
- Area
- Network

- Two or three interfaces depending on the router
- Priority for DR (Router1) and BDR (Router2)
- Redistribute for ASBR (Router3)

This section includes:

- Configuring OSPF on Router1
- Configuring OSPF on Router2
- Configuring OSPF on Router3

Configuring OSPF on Router1

Router1 has a very high priority to ensure it becomes the DR for this area. Also Router1 has the lowest IP address to help ensure it will win in case there is a tie at some point. Otherwise it is a standard OSPF configuration. Setting the priority can only be done in the CLI, and it is for a specific OSPF interface.

To configure OSPF on Router1 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Set **Router ID** to `10.11.101.1` and select **Apply**.
3. In **Areas**, select **Create New,** set the following information, and select **OK**.

Area	0.0.0.0
Type	Regular
Authentication	none

4. In **Networks**, select **Create New**, set the following information, and select **OK**.

IP/Netmask	10.11.0.0/255.255.0.0
Area	0.0.0.0

5. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	Router1-Internal-DR
Interface	port1 (Internal)
IP	0.0.0.0
Authentication	none
Timers (seconds)	
Hello Interval	10
Dead Interval	40

6. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name		Router1-External
Interface		port2 (External)
IP		0.0.0.0
Authentication		none
Timers (seconds)		
	Hello Interval	10
	Dead Interval	40

7. Using the CLI, enter the following commands to set the priority for the Router1-Internal OSPF interface to maximum, ensuring this interface becomes the DR.

```
config router ospf
   config ospf-interface
      edit Router1-Internal-DR
         set priority 255
      end
```

To configure OSPF on Router1 - CLI

```
config router ospf
   set router-id 10.11.101.1
   config area
      edit 0.0.0.0
      next
   end
   config network
      edit 1
         set prefix 10.11.0.0/255.255.255.0
      next
   end
   config ospf-interface
      edit "Router1-Internal"
         set interface "port1"
         set priority 255
      next
      edit "Router1-External"
         set interface "port2"
      next
   end
end
```

Configuring OSPF on Router2

Router2 has a high priority to ensure it becomes the BDR for this area, and configures the DSL interface slightly differently—assume this will be a slower connection resulting in the need for longer timers, and a higher cost for this route.

Otherwise it is a standard OSPF configuration.

To configure OSPF on Router2 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Set **Router ID** to `10.11.101.2` and select **Apply**.
3. In **Areas**, select **Create New**, set the following information, and select **OK**.

Area	0.0.0.0
Type	Regular
Authentication	none

4. In **Networks**, select **Create New**, set the following information, and select **OK**.

IP/Netmask	10.11.0.0/255.255.0.0
Area	0.0.0.0

5. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Router2-Internal
Interface	port1 (Internal)
IP	0.0.0.0
Authentication	none
Timers (seconds)	
Hello Interval	10
Dead Interval	40

6. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	Router2-External
Interface	port2 (External)
IP	0.0.0.0
Authentication	none
Timers (seconds)	
Hello Interval	10
Dead Interval	40

7. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name		Router2-DSL
Interface		port3 (DSL)
IP		0.0.0.0
Authentication		none
Cost		50
Timers (seconds)		
	Hello Interval	20
	Dead Interval	80

8. Using the CLI, enter the following commands to set the priority for the Router2-Internal OSPF interface to ensure this interface will become the BDR:

```
config router ospf
   config ospf-interface
      edit Router2-Internal
         set priority 250
      next
   end
```

To configure OSPF on Router2 - CLI

```
config router ospf
   set router-id 10.11.101.2
   config area
      edit 0.0.0.0
      next
   end
   config network
      edit 1
         set prefix 10.11.0.0/255.255.0.0
      next
   end
   config ospf-interface
      edit "Router2-Internal"
         set interface "port1"
         set priority 255
      next
      edit "Router2-External"
         set interface "port2"
      next
      edit "Router2-DSL"
         set interface "port3"
         set cost 50
      next
   end
end
```

Configuring OSPF on Router3

Router3 is more complex than the other two routers. The interfaces are straightforward, but this router has to import and export routes between OSPF and BGP. That requirement makes Router3 a border router or ASBR. Also Router3 needs a lower cost on its route to encourage all traffic to the Internet to route through it.

In the advanced OSPF options, Redistribute is enabled for Router3. It allows different types of routes, learned outside of OSPF, to be used in OSPF. Different metrics are assigned to these other types of routes to make them more or less preferred to regular OSPF routes.

To configure OSPF on Router3 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Set **Router ID** to `10.11.101.2` and select **Apply**.
3. Expand **Advanced Options**.
4. In **Redistribute**, set the following information, and select **OK**.

Route type	Redistribute	Metric
Connected	Enable	15
Static	Enable	15
RIP	Disable	n/a
BGP	Enable	5

5. In **Areas**, select **Create New**, set the following information, and select **OK**.

Area	0.0.0.0
Type	Regular
Authentication	none

6. In **Networks**, select **Create New**, set the following information, and select **OK**.

IP/Netmask	10.11.0.0/255.255.0.0
Area	0.0.0.0

7. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	Router3-Internal
Interface	port1 (Internal)
IP	0.0.0.0
Authentication	none
Timers (seconds)	

	Hello Interval	10
	Dead Interval	40

8. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name		Router3-Internal2
Interface		port2 (Internal2)
IP		0.0.0.0
Authentication		none
Timers (seconds)		
	Hello Interval	10
	Dead Interval	40

9. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name		Router3-ISP-BGP
Interface		port3 (ISP-BGP)
IP		0.0.0.0
Authentication		none
Cost		2
Timers (seconds)		
	Hello Interval	20
	Dead Interval	80

10. Using the CLI, enter the following commands to set the priority for the Router3-Internal OSPF interface to ensure this interface will become the BDR.

```
config router ospf
   config ospf-interface
   edit Router3-Internal
      set priority 250
   next
end
```

To configure OSPF on Router3 - CLI

```
config router ospf
   set router-id 10.11.102.3
   config area
      edit 0.0.0.0
      next
   end
```

```
    config network
       edit 1
          set prefix 10.11.0.0/255.255.255.0
       next
       edit 2
          set prefix 172.20.120.0/255.255.255.0
       next
    end
    config ospf-interface
       edit "Router3-Internal"
          set interface "port1"
          set priority 255
       next
       edit "Router3-External"
          set interface "port2"
       next
       edit "Router3-ISP-BGP"
          set interface "port3"
          set cost 2
       next
    end
end
```

Configuring other networking devices

The other networking devices required in this configuration are on the two ISP networks, the BGP network for the main Internet connection, and the DSL backup connection.

In both cases, the ISPs need to be notified of the OSPF network settings including router IP addresses, timer settings, and so on. The ISP will use this information to configure its routers that connect to this OSPF network.

Testing network configuration

Testing the network configuration involves two parts: testing the network connectivity, and testing the OSPF routing.

To test the network connectivity use ping, traceroute, and other network tools.

To test the OSPF routing in this example, refer to the troubleshooting outlined in Basic OSPF example on page 385.

Advanced inter-area OSPF example

This example sets up an OSPF network at a large office. There are three areas, each with two routers. Typically OSPF areas would not be this small, and if they were the areas would be combined into one bigger area. However, the stub area services the accounting department which is very sensitive about their network and do not want any of their network information broadcast through the rest of the company. The backbone area contains the bulk of the company network devices. The regular area was established for various reasons such as hosting the company servers on a separate area with extra security.

One area is a small stub area that has no independent Internet connection, and only one connection to the backbone area. That connection between the stub area and the backbone area is only through a default route. No routes outside the stub area are advertised into that area. Another area is the backbone, which is connected to the other two areas. The third area has the Internet connection, and all traffic to and from the Internet must use

that area's connection. If that traffic comes from the stub area, then that traffic is treating the backbone like a transit area that only uses it to get to another area.

In the stub area, a subnet of computers is running the RIP routing protocol and those routes must be redistributed into the OSPF areas.

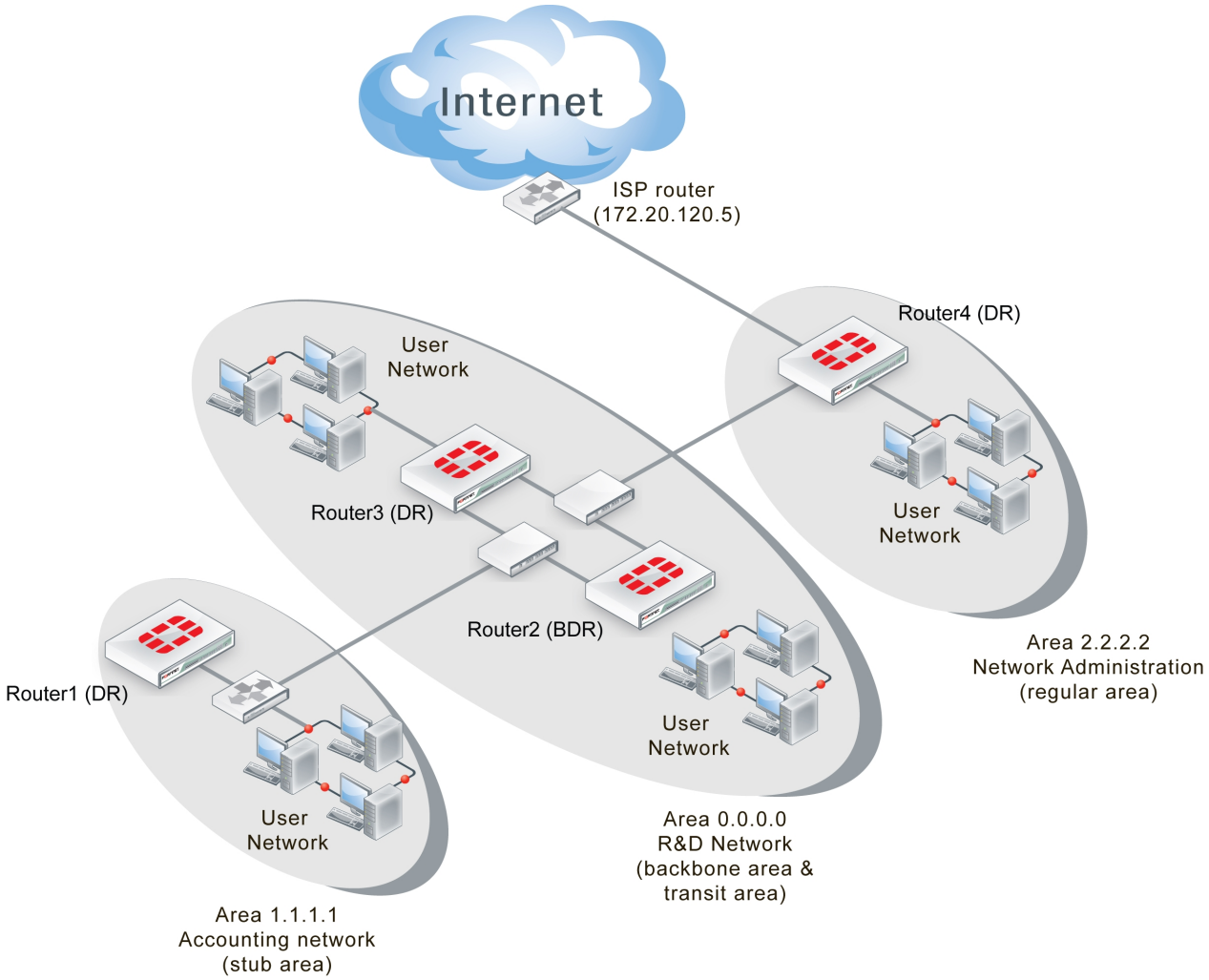
This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate units
- Configuring OSPF on the FortiGate units
- Configuring other networking devices
- Testing network configuration

Network layout and assumptions

There are four FortiGate units in this network topology acting as OSPF routers:

Advanced inter-area OSPF network topology



Area 1.1.1.1 is a stub area with one FortiGate unit OSPF router called Router1 (DR). Its only access outside of that area is a default route to the backbone area, which is how it accesses the Internet. Traffic must go from the stub area, through the backbone, to the third area to reach the Internet. The backbone area in this configuration is called a transit area. Also in area 1.1.1.1 there is a RIP router that will be providing routes to the OSPF area through redistribution.

Area 0.0.0.0 is the backbone area, and has two FortiGate unit routers named Router2 (BDR) and Router3 (DR).

Area 2.2.2.2 is a regular area that has an Internet connection accessed by both the other two OSPF areas. There is only one FortiGate unit router in this area called Router4 (DR). This area is more secure and requires MD5 authentication by routers.

All areas have user networks connected, but they are not important for configuring the network layout for this example.

Internal interfaces are connected to internal user networks only. External1 interfaces are connected to the 10.11.110.0 network, joining Area 1.1.1.1 and Area 0.0.0.0.

External2 interfaces are connected to the 10.11.111.0 network, joining Area 0.0.0.0 and Area 2.2.2.2. The ISP interface is called ISP.

Routers, areas, interfaces, IP addresses for advanced OSPF network

Router name	Area number and type	Interface	IP address
Router1 (DR)	1.1.1.1 - stub area (Accounting)	port1 (internal)	10.11.101.1
		port2 (external1)	10.11.110.1
Router2 (BDR)	0.0.0.0 - backbone area (R&D Network)	port1 (internal)	10.11.102.2
		port2 (external1)	10.11.110.2
		port3 (external2)	10.11.111.2
Router3 (DR)	0.0.0.0 - backbone area (R&D Network)	port1 (internal)	10.11.103.3
		port2 (external1)	10.11.110.3
		port3 (external2)	10.11.111.3
Router4 (DR)	2.2.2.2 - regular area (Network Admin)	port1 (internal)	10.11.104.4
		port2 (external2)	10.11.111.4
		port3 (ISP)	172.20.120.4

Note that other subnets can be added to the internal interfaces without changing the configuration.

Assumptions

- The FortiGate units used in this example have interfaces named port1, port2, and port3.
- All FortiGate units in this example have factory default configuration with FortiOS 5.2 firmware installed, and are in NAT/Route operation mode.
- During configuration, if settings are not directly referred to they will be left at default settings.
- Basic firewalls are in place to allow unfiltered traffic between all connected interfaces in both directions.
- This OSPF network is not connected to any other OSPF areas outside of this example.
- The Internet connection is always available.
- Other devices may be on the network, but do not affect this configuration.

Configuring the FortiGate units

This section configures the basic settings on the FortiGate units to be OSPF routers. These configurations include multiple interface settings, and hostname.

There are four FortiGate units in this example. The two units in the backbone area can be configured exactly the same except for IP addresses, so only router3 (the DR) configuration will be given with notes indicating router2 (the BDR) IP addresses.

Configuring the FortiGate units includes:

- Configuring Router1
- Configuring Router2
- Configuring Router3
- Configuring Router4

Configuring Router1

Router1 is part of the Accounting network stub area (1.1.1.1).

To configure Router1 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Next to hostname, select **Change**.
3. Enter a hostname of `Router1`, and select **OK**.
4. Go to **System > Network > Interfaces,** edit port1, set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.1/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Accounting network
Administrative Status	Up

5. Edit port2, set the following information, and select **OK**.

Alias	External1
IP/Network Mask	10.11.110.1/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Backbone network and Internet
Administrative Status	Up

Configuring Router2

Router2 is part of the R&D network backbone area (0.0.0.0). Router2 and Router3 are in this area. They provide a redundant connection between area 1.1.1.1 and area 2.2.2.2.

Router2 has three interfaces configured; one to the internal network, and two to Router3 for redundancy.

To configure Router2 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Next to hostname, select **Change**.
3. Enter a hostname of `Router2`, and select **OK**.
4. Go to **System > Network > Interfaces**, edit port1 (internal), set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.102.2/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

5. Edit port2 (external1), set the following information, and select **OK**.

Alias	external1
IP/Network Mask	10.11.110.2/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router3 first connection
Administrative Status	Up

6. Edit port3 (external2), set the following information, and select **OK**.

Alias	external2
IP/Network Mask	10.11.111.2/255.255.255.0

Administrative Access	HTTPS SSH PING
Description	Router3 second connection
Administrative Status	Up

Configuring Router3

Router3 is part of the R&D network backbone area (0.0.0.0). Router2 and Router3 are in this area. They provide a redundant connection between area 1.1.1.1 and area 2.2.2.2.

To configure Router3 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Next to hostname, select **Change**.
3. Enter a hostname of `Router3`, and select **OK**.
4. Go to **System > Network > Interfaces**, edit port1 (internal), set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.103.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

5. Edit port2 (external1), set the following information, and select **OK**.

Alias	external1
IP/Network Mask	10.11.110.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router2 first connection
Administrative Status	Up

6. Edit port3 (external2), set the following information, and select **OK**.

Alias	external2
IP/Network Mask	10.11.111.3/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Router2 second connection
Administrative Status	Up

Configuring Router4

Router4 is part of the Network Administration regular area (2.2.2.2). This area provides Internet access for both area 1.1.1.1 and the backbone area.

This section configures interfaces and hostname.

To configure Router4 interfaces - web-based manager

1. Go to **System > Dashboard > Status**.
2. Next to hostname, select **Change**.
3. Enter a hostname of `Router4`, and select **OK**.
4. Go to **System > Network > Interfaces**.
5. Edit port1 (internal).
6. Set the following information, and select **OK**.

Alias	internal
IP/Network Mask	10.11.101.4/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Accounting network
Administrative Status	Up

7. Edit port2 (external2).
8. Set the following information, and select **OK**.

Alias	external2
IP/Network Mask	10.11.110.4/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	Backbone and Accounting network
Administrative Status	Up

9. Edit port3 (ISP).
10. Set the following information, and select **OK**.

Alias	ISP
IP/Network Mask	172.20.120.4/255.255.255.0
Administrative Access	HTTPS SSH PING
Description	ISP and Internet
Administrative Status	Up

Configuring OSPF on the FortiGate units

Three of the routers are designated routers (DR) and one is a backup DR (BDR). This is achieved through the lowest router ID numbers, or OSPF priority settings.

Also each area needs to be configured as each respective type of area - stub, backbone, or regular. This affects how routes are advertised into the area.

To configure OSPF on Router1 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Enter `10.11.101.1` for the **Router ID** and select **Apply**.
3. In **Areas**, select **Create New,** set the following information, and select **OK**.

Area	1.1.1.1
Type	Stub
Authentication	None

4. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.101.0/255.255.255.0
Area	1.1.1.1

5. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Accounting
Interface	port1 (internal)
IP	10.11.101.1
Authentication	None

6. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Backbone1
Interface	port2 (external1)
IP	10.11.110.1
Authentication	None

To configure OSPF on Router2 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Enter `10.11.102.2` for the **Router ID** and select **Apply**.
3. In **Areas**, select **Create New,** set the following information, and select **OK**.

Area	0.0.0.0
Type	Regular
Authentication	None

4. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.102.2/255.255.255.0
Area	0.0.0.0

5. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.110.2/255.255.255.0
Area	0.0.0.0

6. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.111.2/255.255.255.0
Area	0.0.0.0

7. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	RnD network
Interface	port1 (internal)
IP	10.11.102.2
Authentication	None

8. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Backbone1
Interface	port2 (external1)
IP	10.11.110.2
Authentication	None

9. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Backbone2
Interface	port3 (external2)

IP	10.11.111.2
Authentication	None

To configure OSPF on Router3 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Enter `10.11.103.3` for the **Router ID** and then select **Apply**.
3. In **Areas**, select **Create New, s**et the following information, and then select **OK**.

Area	0.0.0.0
Type	Regular
Authentication	None

4. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.102.3/255.255.255.0
Area	0.0.0.0

5. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.110.3/255.255.255.0
Area	0.0.0.0

6. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.111.3/255.255.255.0
Area	0.0.0.0

7. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	RnD network
Interface	port1 (internal)
IP	10.11.103.3
Authentication	None

8. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Backbone1
Interface	port2 (external1)

IP	10.11.110.3
Authentication	None

9. In **Interfaces**, select **Create New,** set the following information, and select **OK**.

Name	Backbone2
Interface	port3 (external2)
IP	10.11.111.3
Authentication	None

To configure OSPF on Router4 - web-based manager

1. Go to **Router > Dynamic > OSPF**.
2. Enter `10.11.104.4` for the **Router ID** and then select **Apply**.
3. In **Areas**, select **Create New**.
4. Set the following information, and select **OK**.

Area	2.2.2.2
Type	Regular
Authentication	None

5. In **Networks**, select **Create New,** set the following information, and select **OK**.

IP/Netmask	10.11.104.0/255.255.255.0
Area	0.0.0.0

6. In **Networks**, select **Create New**, set the following information, and select **OK**.

IP/Netmask	10.11.111.0/255.255.255.0
Area	0.0.0.0

7. In **Networks**, select **Create New**, set the following information, and select **OK**.

IP/Netmask	172.20.120.0/255.255.255.0
Area	0.0.0.0

8. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	Network Admin network

Interface	port1 (internal)
IP	10.11.104.4
Authentication	None

9. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	Backbone2
Interface	port2 (external2)
IP	10.11.111.4
Authentication	None

10. In **Interfaces**, select **Create New**, set the following information, and select **OK**.

Name	ISP
Interface	port3 (ISP)
IP	172.20.120.4
Authentication	None

Configuring other networking devices

All network devices on this network are running OSPF routing. The user networks (Accounting, R&D, and Network Administration) are part of one of the three areas.

The ISP needs to be notified of your network configuration for area 2.2.2.2. Your ISP will not advertise your areas externally as they are intended as internal areas. External areas have assigned unique numbers. The area numbers used in this example are similar to the 10.0.0.0 and 192.168.0.0 subnets used in internal networking.

Testing network configuration

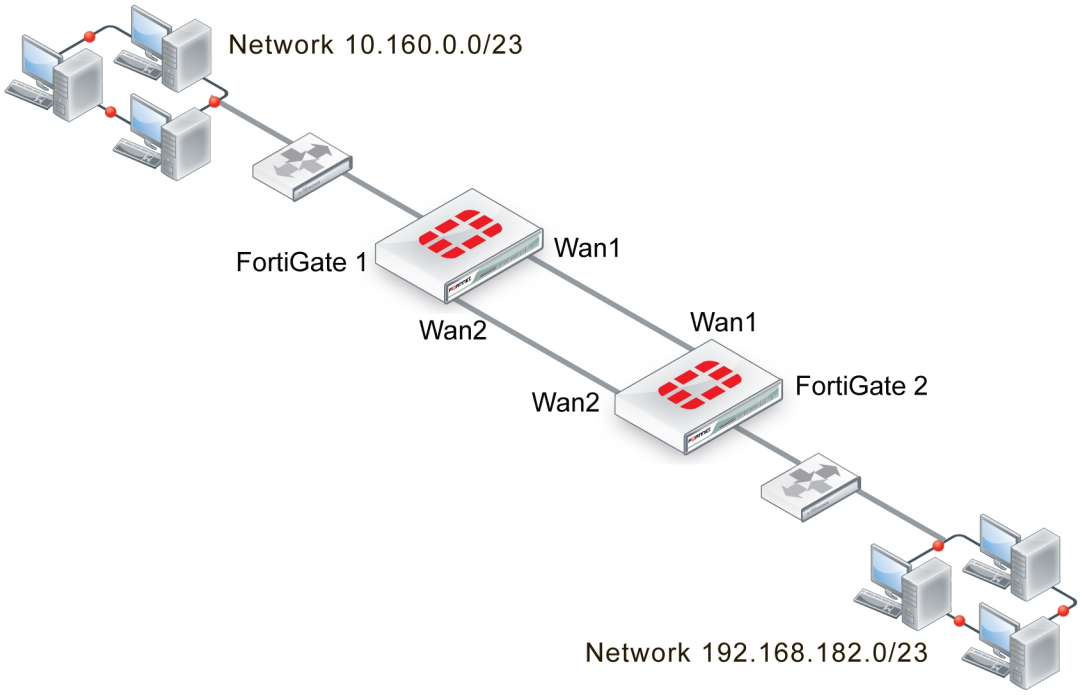
There are two main areas to test in this network configuration; network connectivity, and OSPF routing.

To test the network connectivity, see if computers on the Accounting or R&D networks can access the Internet. If you need to troubleshoot network connectivity, see the FortiOS Handbook Troubleshooting chapter.

To test the OSPF routing, check the routing tables on the FortiGate units to ensure the expected OSPF routes are present. If you need help troubleshooting OSPF routing, see Advanced inter-area OSPF example on page 397.

Controlling redundant links by cost

In this scenario, two FortiGate units have redundant links: one link between their WAN1 interfaces and another between their WAN2 interfaces.



FortiGate 1 should learn the route to network 192.168.182.0 and FortiGate 2 should learn the route to network 10.160.0.0. Under normal conditions, they should learn these routes through the WAN1 link. The WAN2 link should be used only as a backup.

With the default settings, each FortiGate unit learns these routes from both WAN1 and WAN2.

FortiGate 1:

```
FGT1 # get router info ospf neighbor
OSPF process 0:
Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 1 Full/Backup 00:00:33 10.182.0.187 wan1
10.2.2.2 1 Full/Backup 00:00:31 10.183.0.187 wan2
FGT1 # get router info routing-table ospf
O*E2 0.0.0.0/0 [110/10] via 10.183.0.187, wan2, 00:00:01
[110/10] via 10.182.0.187, wan1, 00:00:01
O 192.168.182.0/23 [110/20] via 10.183.0.187, wan2, 00:02:04
[110/20] via 10.182.0.187, wan1, 00:02:04
```

FortiGate 2:

```
FGT2 # get router info ospf neighbor
OSPF process 0:
Neighbor ID Pri State Dead Time Address Interface
10.1.1.1 1 Full/DR 00:00:38 10.182.0.57 wan1
10.1.1.1 1 Full/DR 00:00:38 10.183.0.57 wan2
FGT2 # get router info routing-table ospf
O 10.160.0.0/23 [110/20] via 10.183.0.57, wan2, 00:00:39
[110/20] via 10.182.0.57, wan1, 00:00:39
```

Adjusting the route costs

On both FortiGate units, the cost of the route through WAN2 is adjusted higher so that this route will only be used if the route through WAN1 is unavailable. The default cost is 10. The WAN2 route will be changed to a cost of 200.

On both FortiGate units:

```
config router ospf
   config ospf-interface
      edit "WAN2_higher_cost"
         set cost 200
         set interface "wan2"
      end
```

Now both FortiGate units use only the WAN1 route:

FortiGate 1:

```
FGT1 # get router info routing-table ospf
O*E2 0.0.0.0/0 [110/10] via 10.182.0.187, wan1, 00:00:40
O 192.168.182.0/23 [110/20] via 10.182.0.187, wan1, 00:00:40
```

FortiGate 2:

```
FGT2 # get router info routing-table ospf
O 10.160.0.0/23 [110/20] via 10.182.0.57, wan1, 00:09:37
```

LSDB check on FortiGate 1:

```
FGT1 # get router info ospf database router lsa
Router Link States (Area 0.0.0.0)
LS age: 81
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x0
LS Type: router-LSA
Link State ID: 10.1.1.1
Advertising Router: 10.1.1.1
LS Seq Number: 8000000b
Checksum: 0xe637
Length: 60
Number of Links: 3

   Link connected to: Stub Network
   (Link ID) Network/subnet number: 10.160.0.0
   (Link Data) Network Mask: 255.255.254.0
   Number of TOS metrics: 0
   TOS 0 Metric: 10
   Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.183.0.187
   (Link Data) Router Interface address: 10.183.0.57
   Number of TOS metrics: 0
   TOS 0 Metric: 200

   Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.182.0.57
   (Link Data) Router Interface address: 10.182.0.57
```

```
   Number of TOS metrics: 0
   TOS 0 Metric: 10

LS age: 83
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x2 : ASBR
LS Type: router-LSA
Link State ID: 10.2.2.2
Advertising Router: 10.2.2.2
LS Seq Number: 8000000e
Checksum: 0xfc9b
Length: 60
   Number of Links: 3

   Link connected to: Stub Network
   (Link ID) Network/subnet number: 192.168.182.0
   (Link Data) Network Mask: 255.255.254.0
   Number of TOS metrics: 0
   TOS 0 Metric: 10

   Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.183.0.187
   (Link Data) Router Interface address: 10.183.0.187
   Number of TOS metrics: 0
   TOS 0 Metric: 200

   Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.182.0.57
   (Link Data) Router Interface address: 10.182.0.187
   Number of TOS metrics: 0
   TOS 0 Metric: 10
```

Verifying route redundancy

Bring down WAN1 and then check the routes on the two FortiGate units.

FortiGate 1:

```
FGT1 # get router info routing-table ospf
FGT1 # get router info routing-table ospf
O*E2 0.0.0.0/0 [110/10] via 10.183.0.187, wan2, 00:00:06
O 192.168.182.0/23 [110/210] via 10.183.0.187, wan2, 00:00:06
```

FortiGate 2:

```
FGT2 # get router info routing-table ospf
O 10.160.0.0/23 [110/210] via 10.183.0.57, wan2, 00:00:14
```

The WAN2 interface is now in use on both units.

Intermediate System to Intermediate System Protocol (IS-IS)

This section describes the Intermediate System to Intermediate System Protocol (IS-IS).

The following topics are included in this section:

IS-IS background and concepts
How IS-IS works
Troubleshooting IS-IS
Simple IS-IS example
Network layout and assumptions
Expectations
CLI configuration
Verification
Troubleshooting

IS-IS background and concepts

Intermediate System to Intermediate System Protocol (IS-IS) allows routing of ISO's OSI protocol stack Connectionless Network Service (CLNS). IS-IS is an Interior Gateway Protocol (IGP) not intended to be used between Autonomous Systems (ASes).

Background

IS-IS was developed by Digital Equipment Corporation and later standardized by ISO in 1992 as ISO 19589 (see RFC 1142—note this RFC is different from the ISO version). At roughly the same time, the Internet Engineering Task Force developed OSPF (see Open Shortest Path First (OSPF) on page 371). After the initial version, IP support was added to IS-IS and this version was called Integrated IS-IS (see RFC 1195). Its widespread use started when an early version of IS-IS was included with BSD v4.3 Linux as the routed daemon. The routing algorithm used by IS-IS, the Bellman–Ford algorithm, first saw widespread use as the initial routing algorithm of the ARPANET.

IS-IS is a link state protocol well-suited to smaller networks that is in widespread use and has near universal support on routing hardware. It is quick to configure, and works well if there are no redundant paths. However, IS-IS updates are sent out node-by-node, so it can be slow to find a path around network outages. IS-IS also lacks good authentication, can not choose routes based on different quality of service methods, and can create network loops if you are not careful. IS-IS uses Djikstra's algorithm to find the best path, like OSPF.

While OSPF is more widely known, IS-IS is a viable alternative to OSPF in enterprise networks and ISP infrastructures, largely due to its native support for IPv6 and its non-disruptive methods for splitting, merging, migrating, and renumbering network areas.

The FortiGate implementation supports IS-IS for IPv4 (see RFCs 1142 and 1162), but does not support IS-IS for IPv6 (although this technically can be achieved using the ZebOS routing module).

How IS-IS works

As one of the original modern dynamic routing protocols, IS-IS is straightforward. Its routing algorithm is not complex, there are some options to allow fine tuning, and it is straightforward to configure IS-IS on FortiGate units.

From RFC 1142:

> *The routing algorithm used by the Decision Process is a shortest path first (SPF) algorithm. Instances of the algorithm are run independently and concurrently by all intermediate systems in a routing domain. IntraDomain routing of a PDU occurs on a hop-by-hop basis: that is, the algorithm determines only the next hop, not the complete path, that a data PDU will take to reach its destination.*

IS-IS versus static routing

IS-IS was one of the earliest dynamic routing protocols to work with IP addresses. As such, it is not as complex as more recent protocols. However, IS-IS is a big step forward from simple static routing.

While IS-IS may be slow in response to network outages, static routing has zero response. The same is true for convergence—static routing has zero convergence. Both IS-IS and static routing have the limited hop count, so it is neither a strength nor a weakness.

TLV

IS-IS uses *type-length-variable (TLV)* parameters to carry information in Link-State PDUs (LSPs). Each IS-IS LSP consists of a variable-length header to which TLVs are appended in order to extend IS-IS for IP routing. The TLV field consists of one octet of type (T), one octet of length (L), and "L" octets of Value (V). They are included in all of the IS-IS Packet types. For a complete breakdown of the LSP, see LSP structure on page 413.

In IS-IS, TLVs are used to determine route-leaking and authentication, and are also used for IPv4 and IPv6 awareness and reachability.

- To determine which TLVs are responsible for route-leaking, see Default routing on page 416.
- To determine which TLVs are responsible for authentication, see Authentication on page 417.

For a complete list of reserved TLV codepoints, refer to RFC 3359.

LSP structure

It is difficult to fully understand a routing protocol without knowing what information is carried in its packets. Knowing how routers exchange each type of information will help you better understand the IS-IS protocol and will allow you to configure your network more appropriatey.

This section provides information on the contents of the IS-IS LSP. LSPs describe the network topology and can include IP routes and checksums.

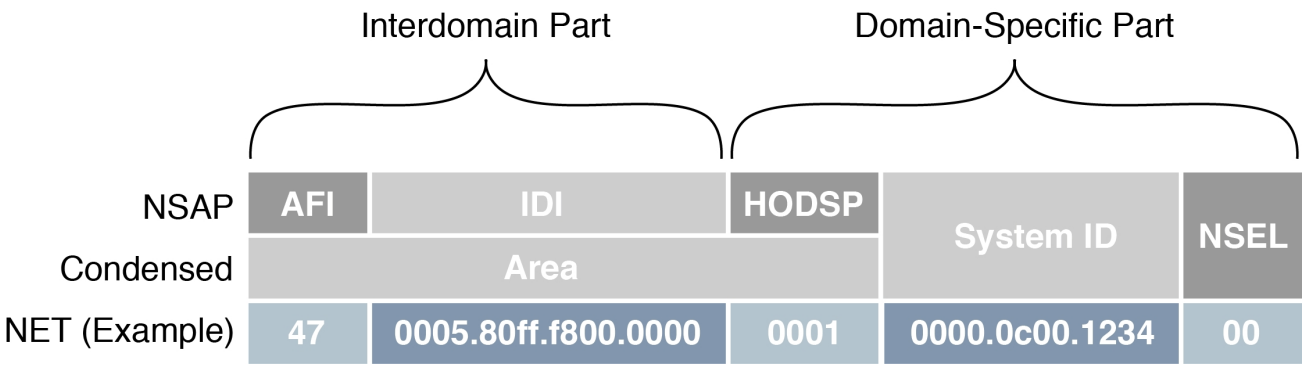
NSAP and NET

IS-IS routing protocol utilizes ISO network addressing to identify network interfaces. The addresses are known as Network Service Access Points (NSAPs). In general, IS-IS routers consist of only one NSAP, whereas IP addressing requires one IP address per interface.

In IS-IS, the NSAP address is translated into a Network Entity Title (NET), which is the same as the NSAP but can differentiate end systems by way of a byte called the *n-selector* (NSEL). In order for adjacencies to form in IS-IS, the NSEL must necessarily be set to zero, to indicate “this system”. The total NET can be anywhere between 8 and 20 bytes long due to the support for variable length area addressing.

The following diagram identifies the individual parts of the NSAP, with explanations below.

NSAP and NET example



AFI — The *Authority and Format Identifier (AFI)* specifies the format of the addressing family used. IS-IS is designed to carry routing information for several different protocols. Each entry has an address family identifier that identifies the globally unique Interdomain Part (IDP). For example, 49 is the AFI for private addresses, whereas 47 is the AFI for international organizations.

IDI — The *Initial Domain Identifier (IDI)* identifies the routing domain within an interconnected network. The length of the IDI is typically determined by the AFI. If you are using an AFI of 49, you do not need to specify an IDI, since the network is private.

HODSP — The *High Order Domain-Specific Part (HODSP)* identifies the unique address within a specific routing domain. Together, the AFI, IDI, and HODSP define the area address. All of the nodes within an area must have the same area address.

System ID — The *System ID* represents the 6-8 byte router identifier. The ID could be Media Access Control (MAC) format, as in the example above, or a static length IP address expressed in binary-coded decimal (BCD) format.

NSEL — The *n-selector (NSEL)*, as previously described, identifies the network layer transport service and must always be set to zero for IS-IS NETs.

Parts and terminology of IS-IS

Before you can understand how IS-IS functions, you need to understand some of the main concepts and parts of IS-IS.

This section includes:

- DIS election and pseudonode LSP
- Packet types
- Default routing
- Timer options
- Authentication

DIS election and pseudonode LSP

In IS-IS routing protocol, a single router is chosen to be the designated intermediate system (DIS). The election of the DIS is determined automatically and dynamically on the LAN depending on highest interface priority and the subnetwork point of attachment (SNPA). The FortiGate is typically the DIS, and each router in its LAN is an intermediate system (IS).

Unlike OSPF, which elects a designated router (DR) and backup designated router (BDR), the DIS has no backup and determines the election of a new DIS whenever a router is added to the LAN or whenever the current DIS drops. A backup DIS is irrelevant since all of the routers on an IS-IS system are synchronized, and the short Hello interval used by the DIS quickly detects failures and the subsequent replacement of the DIS.

Synchronization of all the nodes in an IS-IS area could prove troublesome when updating the network infrastructure, and would demand ever-increasing resources each time a new router is added (at an exponential scale). For this purpose the DIS creates a pseudonode, which is essentially a virtual, logical node representing the LAN. The pseudonode requests adjacency status from all the routers in a multi-access network by sending IS-IS Hello (IIH) PDUs to Level 1 and Level 2 routers (where Level 1 routers share the same address as the DIS and Level 2 routers do not). Using a pseudonode to alter the representation of the LAN in the link-state database (LSD) greatly reduces the amount of adjacencies that area routers have to report. In essence, a pseudonode *collapses* a LAN topology, which allows a more linear scale to link-state advertising.

In order to maintain the database synchronization, the DIS periodically sends complete sequence number packets (CSNPs) to all participating routers.

Packet types

Four general packet types (PDUs) are communicated through IS-IS, appearing at both Level 1 and Level 2. They are described below.

Intermediate System-to-Intermediate System Hello (IIH) PDU — As mentioned previously, the IIH PDU, or Hello packet, detects neighboring routers and indicates to the pseudonode the area's adjacency mesh. The Hello packet, flooded to the multicast address, contains the system ID of the sending router, the holding time, the circuit type of the interface on which the PDU was sent, the PDU length, the DIS identifier, and the interface priority (used in DIS election). The Hello packet also informs its area routers that it is the DIS.

Hello packets are padded to the maximum IS-IS PDU size of 1492 bytes (the full MTU size) to assist in the detection of transmission errors with large frames or with MTU mismatches between adjacencies.

The DIS typically floods Hello packets to the entire LAN every three seconds.

Link-state PDU (LSP) — The LSP contains information about each router in an area and its connected interfaces. LSPs are refreshed periodically and acknowledged on the network by way of sequence number PDUs. If new LSP information is found, based on the most recent complete sequence number PDU (CSNP), then out-of-date entries in the link-state database (LSDB) are removed and the LSDB is updated.

For a more detailed breakdown of the LSP, see LSP structure on page 413.

Complete sequence number PDU (CSNP) — CSNPs contain a list of all LSPs in the current LSDB. The CSNP informs other area routers of missing or outdated links in the adjacency mesh. The receiving routers then use this information to update their own database to ensure that all area routers converge.

In contrast to Hello packets, CSNPs are sent every ten seconds and only between neighbors. In other words, they are never flooded.

Partial sequence number PDU (PSNP) — PSNPs are used to request and acknowledge LSP information from an adjacency. When a router compares a CSNP with its local database and determines a discrepancy, the router requests an updated LSP using a PSNP. Once received, the router stores the LSP in its local database and responds to the DIS with acknowledgement.

Default routing

The default route is used if either there are no other routes in the routing table or if none of the other routes apply to a destination. Including the gateway in the default route gives all traffic a next-hop address to use when leaving the local network. The gateway address is normally another router on the edge of the local network.

FortiGate units come with a default static route with an IPv4 address of 0.0.0.0, an administration distance of 10, and a gateway IPv4 address. Beginner administrators can use the default route settings until a more advanced configuration is warranted.

By default, all routes are displayed in the Routing Monitor list. To display the routes in the routing table, go to **Router > Monitor > Routing Monitor**.

Route leaking

Route leaking is the term used to describe the bi-directional flow of information between internal and external routing interfaces. By default, IS-IS leaks routing information from a Level 1 area into a Level 2 area. In order to leak Level 2 routing information into a Level 1 area, you must configure an export policy. Whether or not a route is leaked is determined by the ATT bit, using TLV 128 (for internal IP reachability) and TLV 130 (for external IP address information). For more information on TLVs, see Troubleshooting IS-IS on page 418.

To configure IS-IS route leaking, use the following CLI commands.

1. On a Level 1-2 router:

```
config router isis
   set redistribute-l2 enable
end
```

2. On a Level 1 router:

```
config router isis
   get router info routing-table isis
   get router info isis route
end
```

Default information originate option

Enabling default-information-originate generates and advertises a default route into the FortiGate unit's IS-IS-enabled networks. The generated route may be based on routes learned through a dynamic routing protocol, routes in the routing table, or both. IS-IS does not create the default route unless you use the `always` option.

Select **Disable** if you experience any issues or if you wish to advertise your own static routes into IS-IS updates.

The CLI commands associated with default information originate include:

```
config router isis
   set default-originate
end
```

Timer options

IS-IS uses various timers to regulate its performance including a garbage timer, update timer, and timeout timer. The FortiGate unit default timer settings (30, 180, and 120 seconds respectively) are effective in most configurations—if you change these settings, ensure that the new settings are compatible with local routers and access servers.

You can configure the three IS-IS timers in the CLI, using the following commands:

```
config router isis
   set garbage-timer
   set update-timer
   set timeout-timer
end
```

You will find more information on each timer below.

Update timer

The update timer determines the interval between routing updates. Generally, this value is set to 30 seconds. There is some randomness added to help prevent network traffic congestion, which could result from all routers simultaneously attempting to update their neighbors. The update timer should be at least three times smaller than the timeout timer, otherwise you will experience an error.

If you are experiencing significant traffic on your network, you can increase this interval to send fewer updates per minute. However, ensure you increase the interval for all the routers on your network or you will experience timeouts that will degrade your network speed.

Timeout timer

The timeout timer is the maximum amount of time (in seconds) that a route is considered reachable while no updates are received for the route. This is the maximum time the DIS will keep a reachable route in the routing table while no updates for that route are received. If the DIS receives an update for the route before the timeout period expires, the timer is restarted. The timeout period should be at least three times longer than the update period, otherwise you will experience an error.

If you are experiencing problems with routers not responding in time to updates, increase this timer. However, remember that longer timeout intervals result in longer overall update periods — it may be considerable time before the DIS is done waiting for all the timers to expire on unresponsive routes.

Garbage timer

The garbage timer is the amount of time (in seconds) that the DIS will advertise a route as being unreachable before deleting the route from the routing table. If this timer is shorter, it will keep more up-to-date routes in the routing table and remove old ones faster. This results in a smaller routing table which is useful if you have a very large network, or if your network changes frequently.

Authentication

In routing protocols, it is typically desireable to establish authentication rules that prevent malicious and otherwise unwanted information from being injected into the routing table. IS-IS routing protocol utilizes TLV 10 to establish authentication. For more information on TLVs, see TLV on page 413.

Initially, IS-IS used plain Clear Text to navigate the authentication rules, but this was found to be insecure since the Clear Text packets were unencrypted and could be exposed to packet sniffers. As per RFC 3567, HMAC-MD5 and Enhanced Clear Text authentication features were introduced to IS-IS, both of which encrypt authentication data, making them considerably more secure than using plain Clear Text authentication.

HMAC-MD5 authentication

Hashed Message Authentication Codes - Message Digest 5 (HMAC-MD5) is a mechanism for applying a cryptographic hash function to the message authentication process. It is applied at both Level 1 and Level 2 routing. In IS-IS, an HMAC-MD5 can be applied to each type of LSP, on different interfaces, and with different passwords.

Authentication data is hashed using an AH (Authentication Header) key. From RFC 2085:

> *The "AH Key" is used as a shared secret between two communicating parties. The Key is not a "cryptographic key" as used in a traditional sense. Instead, the AH key (shared secret) is hashed with the transmitted data and thus, assures that an intervening party cannot duplicate the authentication data. [...] Implementation should, and as frequently as possible, change the AH key. Keys need to be chosen at random, or generated using a cryptographically strong pseudo-random generator seeded with a random seed."*

Clear Text authentication uses the configuration commands `area-password` and `domain-password` for authentication, but when migrating from Clear Text authentication to HMAC-MD5, these command settings are automatically overwritten.

By the year 2005, the MD5 hash function had been identified as vulnerable to collision search attacks and various weaknesses. While such vulnerabilities do not compromise the use of MD5 within HMAC, administrators need to be aware of potential developments in cryptanalysis and cryptographic hash functions in the likely event that the underlying hash function needs to be replaced.

Enhanced Clear Text authentication

Enhanced Clear Text authentication is an extension to Clear Text authentication that allows the encryption of passwords as they are displayed in the configuration. It includes a series of authentication mode commands and an authentican key chain, and allows for more simple password modification and password management. Enhanced Clear Text authentication also provides for smoother migration to and from changing authentication types. Intermediate systems continue to use the original authentication method until all the area routers are updated to use the new method.

Authentication key chain

A key chain is a list of one or more authentication keys including the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. A router migrates from one key to the next according to the scheduled send and receive lifetimes. If an active key is unavailable, then the PDU is automatically discarded.

From RFC 5310:

> *It should be noted that the cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function and on the size and quality of the key.*

Troubleshooting IS-IS

This section includes:

- Routing loops
- Split horizon and Poison reverse updates

Routing loops

Normally in routing, a path between two addresses is chosen and traffic is routed along that path from one address to the other. When there is a routing loop, that normal path doubles back on itself creating a loop. When there are loops, the network has problems.

A routing loop happens when a normally functioning network has an outage, and one or more routers are offline. When packets encounter this, an alternate route is attempted to maneuver around the outage. During this phase it is possible for a route to be attempted that involves going back a hop, and trying a different hop forward. If that hop forward is blocked by the outage as well, a hop back and possibly the original hop forward may be selected. You can see if this continues, how it can consume not only network bandwidth but also many resources on those routers affected. The worst part is this situation will continue until the network administrator changes the router settings, or the downed routers come back online.

Routing loop effect on the network

In addition to this “traffic jam” of routed packets, every time the routing table for a router changes that router sends an update out to all of the IS-IS routers connected to it. In a network loop, its possible for a router to change its routes very quickly as it tries and fails along these new routes. This can quickly result in a flood of updates being sent out, which can effectively grind the network to a halt until the problem is fixed.

How can you spot a routing loop

Any time network traffic slows down, you will be asking yourself if it is a network loop or not. Often slowdowns are normal, they are not a full stoppage, and normal traffic resumes in a short period of time.

If the slow down is a full halt of traffic or a major slowdown does not return to normal quickly, you need to do serious troubleshooting quickly.

Some methods to troubleshoot your outage include:

- Checking your logs
- Using SNMP network monitoring
- Using Link Health Monitor and e-mail alerts
- Looking at the packet flow

If you aren’t running SNMP, dead gateway detection, or you have non-Fortinet routers in your network, you can use networking tools such as ping and traceroute to define the outage on your network and begin to fix it.

Checking your logs

If your routers log events to a central location, it can be easy to check the logs for your network for any outages.

On your FortiGate unit, go to **Log & Report > Log & Archive Access**. You will want to look at both event logs and traffic logs. Events to look for will generally fall under CPU and memory usage, interfaces going offline (due to dead gateway detection), and other similar system events.

Once you have found and fixed your network problem, you can go back to the logs and create a report to better see how things developed during the problem. This type of forensics analysis can better help you prepare for next time.

Using SNMP network monitoring

If your network had no problems one minute and slows to a halt the next, chances are something changed to cause that problem. Most of the time an offline router is the cause, and once you find that router and bring it back online, things will return to normal.

If you can enable a hardware monitoring system such as SNMP or sFlow on your routers, you can be notified of the outage and where it is exactly as soon as it happens.

Ideally you can configure SNMP on all your FortiGate routers and be alerted to all outages as they occur.

To use SNMP to detect potential routing loops

1. Go to **System > Config > SNMP**.
2. Enable **SNMP Agent**.
3. Optionally enter the **Description**, **Location**, and **Contact** information for this device for easier location of the problem report.
4. In either **SNMP v1/v2c** section or **SNMP v3** section, as appropriate, select **Create New**.
5. Enter the **Community Name** that you want to use.
6. In **Hosts**, select Add to add an IP address where you will be monitoring the FortiGate unit. You can add up to 8 different addresses.
7. Ensure that ports 161 and 162 (SNMP queries and traps) are allowed through your security policies.
8. In **SNMP Event**, select the events you want to be notified of. For routing loops this should include **CPU Overusage**, **Memory Low**, and possibly **Log disk space low**. If there are problems, the log will be filling up quickly, and the FortiGate unit's resources will be overused.
9. Select **OK**.
10. Configure SNMP host (manager) software on your administration computer. This will monitor the SNMP information sent out by the FortiGate unit. Typically you can configure this software to alert you to outages or CPU spikes that may indicate a routing loop.

Using Link Health Monitor and e-mail alerts

Another tool available to you on FortiGate units is the Link Health Monitor, useful for dead gateway detection. This feature allows the FortiGate unit to ping a gateway at regular intervals to ensure it is online and working. When the gateway is not accessible, that interface is marked as down.

To detect possible routing loops with Link Health Monitor

1. To configure dead gateway detection, go to **Router > Static > Settings** and select **Create New**.
2. Set the **Probe Interval** (how often to send a ping), and **Failure Threshold** (how many lost pings is considered a failure). A smaller interval and smaller number of lost pings will result in faster detection, but will create more traffic on your network.
3. You may also want to log CPU and Memory usage as a network outage will cause your CPU activity to spike.

If you have VDOMs configured, you will have to enter the basic SMTP server information in the Global section, and the rest of the configuration within the VDOM that includes this interface.

After this configuration, when this interface on the FortiGate unit cannot connect to the next router, the FortiGate unit will bring down the interface and alert you with an email to the outage.

Looking at the packet flow

If you want to see what is happening on your network, look at the packets travelling on the network. In this situation, you are looking for routes that have metrics higher than 15 as that indicates they are unreachable. Ideally if you debug the flow of the packets, and record the routes that are unreachable, you can create an accurate picture of the network outage.

Action to take on discovering a routing loop

Once you have mapped the problem on your network, and determined it is in fact a routing loop there are a number of steps to take in correcting it.

1. Get any offline routers back online. This may be a simple reboot, or you may have to replace hardware. Often this first step will restore your network to its normal operation, once the routing tables finish being updated.
2. Change your routing configuration on the edges of the outage. Even if step 1 brought your network back online, you should consider making changes to improve your network before the next outage occurs. These changes can include configuring features like holddowns and triggers for updates, split horizon, and poison reverse updates.

Split horizon and Poison reverse updates

Split horizon is best explained with an example. You have three routers linked serially, let's call them A, B, and C. A is only linked to B, C is only linked to B, and B is linked to both A and C. To get to C, A must go through B. If the link to C goes down, it is possible that B will try to use A's route to get to C. This route is A-B-C, so it will not work. However, if B tries to use it this begins an endless loop.

This situation is called a split horizon because from B's point of view the horizon stretches out in each direction, but in reality it only is on one side.

Poison reverse is the method used to prevent routes from running into split horizon problems. Poison reverse "poisons" routes away from the destination that use the current router in their route to the destination. This "poisoned" route is marked as unreachable for routers that cannot use it. In IS-IS this means that route is marked with a distance of 16.

Simple IS-IS example

This is an example of a typical medium-sized network configuration using IS-IS routing.

Imagine a company with four FortiGate devices connected to one another. A FortiGate at one end of the network connects to two routers, each with its own local subnet; one of these routers uses OSPF and the other uses RIP.

Your task is to configure the four FortiGates to route traffic and process network updates using IS-IS, such that the farthest FortiGate (see 'FGT4' in Network layout and assumptions on page 422) receives route updates for the two routers at the opposite end of the network. Furthermore, FGT4 has been given a loopback subnet that must be identified by the router running RIP.

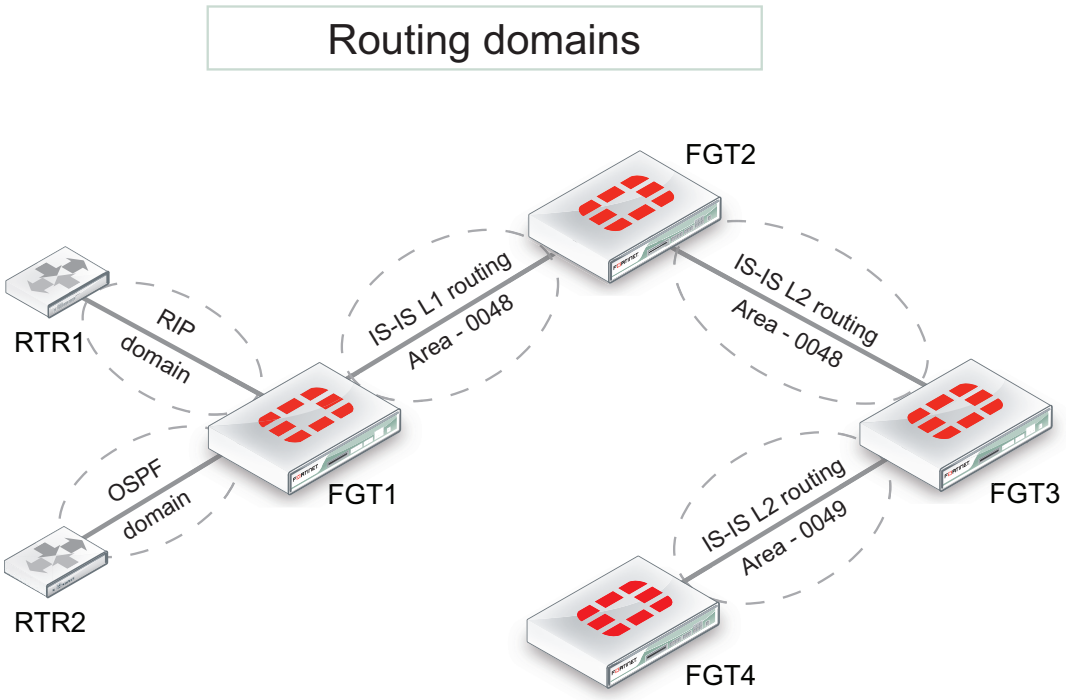
Since the internal networks use OSPF and RIP, those protocols will need to be redistributed through the IS-IS network. To keep the example simple, there will be no authentication of router traffic.

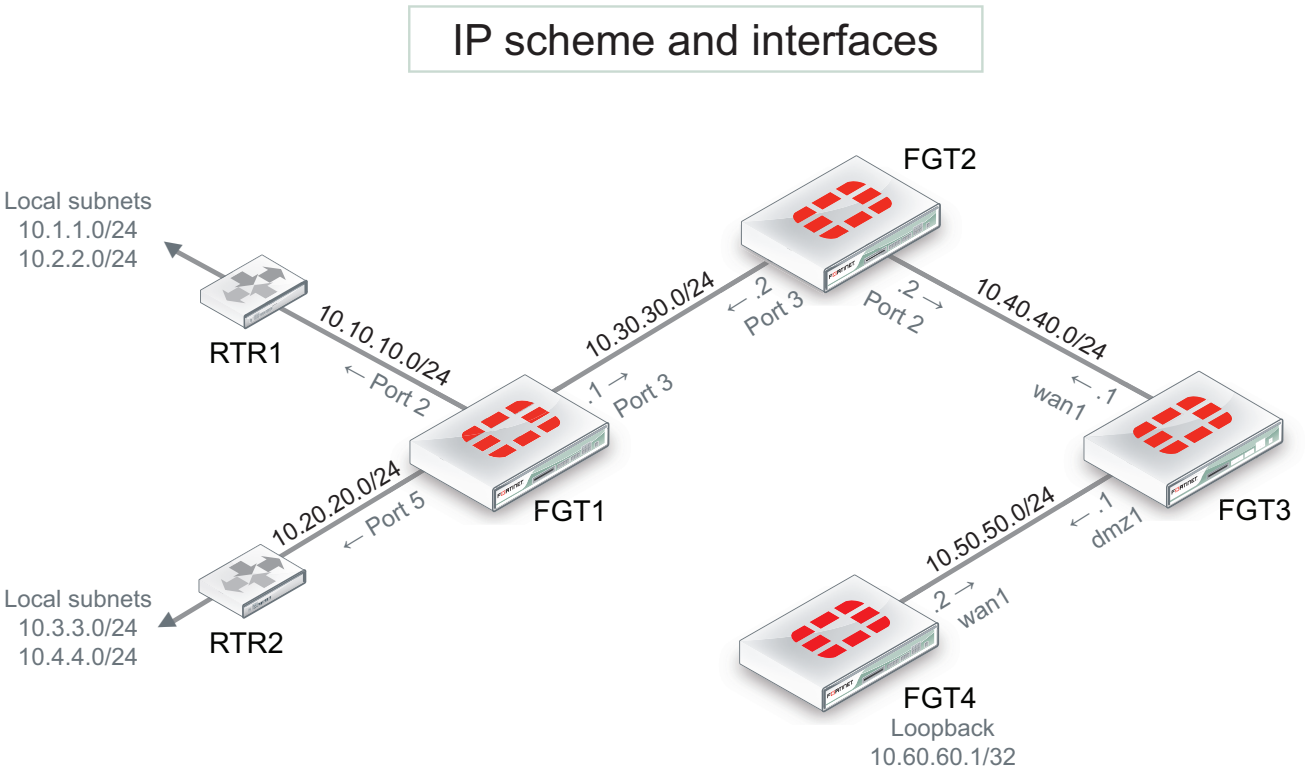
With IS-IS properly configured in this example, if a router fails or temporarily goes offline, the route change will propagate throughout the system.

This section includes the following topics:

- Network layout and assumptions
- Expectations
- CLI configuration
- Verification
- Troubleshooting

Network layout and assumptions





- It is assumed that each FortiGate is operating in NAT mode, running FortiOS 5.2.
- All interfaces have been previously assigned and no static routes are required.
- The AFI (Authority and Format Identifier) used is 49 : Locally administered (private).
- The Area identifiers are 0048 and 0049.

Expectations

- FGT4 must get the IS-IS route updates for RTR1 and RTR2 local subnets (10.1.1.0, 10.2.2.0, 10.3.3.0, 10.4.4.0).
- RTR1 must receive (via RIP2) the loopback subnet of FGT4 (10.60.60.1/32).

CLI configuration

The following CLI configuration occurs on each FortiGate (as identified), including only the relevant parts.

FGT1

```
config router isis
   config isis-interface
      edit "port3"
         set circuit-type level-1
         set network-type broadcast
         set status enable
      next
   end
   config isis-net
      edit 1
         set net 49.0048.1921.6818.2136.00
      next
```

```
      end
      config redistribute "connected"
      end
      config redistribute "rip"
         set status enable
         set level level-1
      end
      config redistribute "ospf"
         set status enable
         set level level-1
      end
   end
   config router rip
      config interface
         edit "port2"
            set receive-version 2
            set send-version 2
         next
      end
      config network
         edit 1
            set prefix 10.10.10.0 255.255.255.0
         next
      end
      config redistribute "isis"
         set status enable
      end
   end
```

FGT2

```
   config router isis
      config isis-interface
         edit "port3"
            set circuit-type level-1
            set network-type broadcast
            set status enable
         next
         edit "port2"
            set network-type broadcast
            set status enable
         next
      end
      config isis-net
         edit 1
            set net 49.0048.1221.6818.2110.00
         next
      end
      set redistribute-l1 enable
      set redistribute-l2 enable
   end
```

FGT3

```
   config router isis
```

```
   set is-type level-2-only
      config isis-interface
         edit "wan1"
            set network-type broadcast
            set status enable
         next
         edit "dmz1"
            set network-type broadcast
            set status enable
         next
      end
      config isis-net
         edit 1
            set net 49.0048.1921.6818.2108.00
         next
         edit 2
            set net 49.0049.1921.6818.2108.00
         next
      end
end
```

FGT4

```
config router isis
   set is-type level-2-only
      config isis-interface
         edit "wan1"
            set network-type broadcast
            set status enable
         next
      end
      config isis-net
         edit 1
            set net 49.0049.1721.0160.1004.00
         next
      end
      config redistribute "connected"
         set status enable
      end
end
```

Verification

Once the network has been configured, you need to test that it works as expected. Use the following CLI commands on the devices indicated.

Verifying if RTR1 receives loopback subnet of FGT4

```
(RTR1) # get router info routing-table all
```

Result:

```
C    10.1.1.0/24 is directly connected, vlan1
C    10.2.2.0/24 is directly connected, vlan2
C    10.10.10.0/24 is directly connected, dmz1
```

```
R    10.40.40.0/24 [120/2] via 10.10.10.1, dmz1, 00:04:07
R    10.50.50.0/24 [120/2] via 10.10.10.1, dmz1, 00:04:07
R    10.60.60.1/32 [120/2] via 10.10.10.1, dmz1, 00:04:07
```

(*) If required, filtering out 10.50.50.0 and 10.40.40.0 from the routing table could be done with a route-map.

Verification on FGT2, which is the border between L1 and L2 routing levels; looking at IS-IS information

```
FGT2 # get router info isis interface
```

Result:

```
port2 is up, line protocol is up
Routing Protocol: IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000003
Local SNPA: 0009.0f85.ad8c
IP interface address:
10.40.40.2/24
IPv4 interface address:
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 1221.6818.2110.01
Number of active level-1 adjacencies: 0
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 1221.6818.2110.01
Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-1 Hello in 6 seconds
Next IS-IS LAN Level-2 Hello in 1 seconds
port3 is up, line protocol is up
Routing Protocol: IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000004
Local SNPA: 0009.0f85.ad8d
IP interface address:
10.30.30.2/24
IPv4 interface address:
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 1221.6818.2110.02
Number of active level-1 adjacencies: 1
Next IS-IS LAN Level-1 Hello in 2 seconds

FGT2 # get router info isis neighbor
```

Result:

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
1921.6818.2108	port2	0009.0f04.0794	Up	22	L2	IS-IS
1921.6818.2136	port3	0009.0f85.acf7	Up	29	L1	IS-IS

Verification on FGT3, which is border between 2 areas; looking at IS-IS information

IS-IS router CLI commands available:

```
FGT3 # get router info isis ?
```

Result:

```
interface                       show isis interfaces
neighbour                       show CLNS neighbor adjacencies
is-neighbour                    show IS neighbor adjacencies
database                        show IS-IS link state database
route                           show IS-IS IP routing table
topology                        show IS-IS paths
```

Example of interface status and neighbors:

```
FGT3 # get router info isis interface
```

Result:

```
wan1 is up, line protocol is up
Routing Protocol: IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000003
Local SNPA: 0009.0f04.0794
IP interface address:
10.40.40.1/24
IPv4 interface address:
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 1221.6818.2110.01
Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-2 Hello in 3 seconds

dmz1 is up, line protocol is up
Routing Protocol: IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1-2
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000005
Local SNPA: 0009.0f04.0792
IP interface address:
10.50.50.1/24
IPv4 interface address:
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 1721.0160.1004.01
Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-2 Hello in 7 seconds
```

```
FGT3 # get router info isis neighbor
```

Result:

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
1221.6818.2110	wan1	0009.0f85.ad8c	Up	8	L2	IS-IS
1721.0160.1004	dmz1	0009.0f52.7704	Up	8	L2	IS-IS

Verification on FGT4 that the remote subnets from RTR1 and RTR2 are in the routing table and learned with IS-IS

```
FGT4 # get router info routing-table all
```

Result:

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

i L2 10.1.1.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.2.2.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.3.3.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.4.4.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46

i L2 10.10.10.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.11.11.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.20.20.0/24 [115/30] via 10.50.50.1, wan1, 00:12:46
i L2 10.30.30.0/24 [115/30] via 10.50.50.1, wan1, 00:13:55
i L2 10.40.40.0/24 [115/20] via 10.50.50.1, wan1, 00:15:30

C 10.50.50.0/24 is directly connected, wan1
C 10.60.60.1/32 is directly connected, loopback

Troubleshooting

The following diagnose commands are available for further IS-IS troubleshooting and will display all IS-IS activity (sent and received packets):

```
FGT # diagnose ip router isis level info
FGT # diagnose ip router isis all enable
FGT # diagnose debug enable
```

…to stop the debug type output:

```
FGT # diagnose ip router isis level none
```

Output and interpretation depends on the issue faced. You can provide this information to TAC if you open a support ticket.

Chapter 4 - Authentication

Change log

Date	Change Description
2017-04-06	Added information regarding fall-through authentication policies.
2016-09-07	Added information regarding user disclaimer page for ethernet interface captive portals.
2016-04-25	Improved diagrams.
2016-04-13	Added RADIUS attribute support, Framed-IP-Address, for SSL VPN authentication.
2016-03-09	Added information re: LDAP user group support in PAP/CHAP protocols. Minor other updates.
2015-12-18	Improved Examples and Troubleshooting on page 599
2015-12-17	Improved Monitoring authenticated users on page 596
2015-12-14	Improved SSO using RADIUS accounting records on page 589
2015-11-09	Improved Agent-based FSSO on page 545
2015-10-29	Improved Single Sign-On to Windows AD on page 537
2015-10-22	Improved Single Sign-On using a FortiAuthenticator unit on page 533
2015-10-14	Improved Certificate-based authentication on page 514
2015-10-09	Improved Captive portals on page 506
2015-10-02	Improved Configuring authenticated access on page 489
2015-09-25	Improved Managing Guest Access on page 483
2015-06-20	Improved Users and user groups on page 463
2015-05-22	Improved Authentication servers on page 440
2015-04-14	Updated Introduction to authentication on page 431
2015-03-31	Initial release.

This Handbook chapter contains the following sections:

Introduction to authentication describes some basic elements and concepts of authentication.

Authentication servers describes external authentication servers, where a FortiGate unit fits into the topology, and how to configure a FortiGate unit to work with that type of authentication server.

Users and user groups describes the different types of user accounts and user groups. Authenticated access to resources is based on user identities and user group membership. Two-factor authentication methods, including FortiToken, provide additional security.

Managing Guest Access explains how to manage temporary accounts for visitors to your premises.

Configuring authenticated access provides detailed procedures for setting up authenticated access in security policies and authenticated access to VPNs.

Captive portals describes how to authenticate users through a web page that the FortiGate unit presents in response to any HTTP request until valid credentials are entered. This can be used for wired or WiFi network interfaces.

Certificate-based authentication describes authentication by means of X.509 certificates.

Single Sign-On using a FortiAuthenticator unit describes how to use a FortiAuthenticator unit as an SSO agent that can integrate with external network authentication systems such as RADIUS and LDAP to gather user logon information and send it to the FortiGate unit. Users can also log on through a FortiAuthenticator-based web portal or the FortiClient SSO Mobility Agent.

Single Sign-On to Windows AD describes how to set up Single Sign-On in a Windows AD network by configuring the FortiGate unit to poll domain controllers for information user logons and user privileges.

Agent-based FSSO describes how to set up Single Sign-On in Windows AD, Citrix, or Novell networks by installing Fortinet Single Sign On (FSSO) agents on domain controllers. The FortiGate unit receives information about user logons and allows access to network resources based on user group memberships.

SSO using RADIUS accounting records describes how to set up Single Sign-On in a network that uses RADIUS authentication. In this configuration, the RADIUS server send RADIUS accounting records to the FortiGate unit when users log on or off the network. The record includes a user group name that can be used in FortiGate security policies to determine which resources each user can access.

Monitoring authenticated users describes FortiOS authenticated user monitor screens.

Examples and Troubleshooting provides configuration examples and troubleshooting suggestions.

Introduction to authentication

Identifying users and other computers—authentication—is a key part of network security. This section describes some basic elements and concepts of authentication.

The following topics are included in this section:

- What is authentication?
- Methods of authentication
- Types of authentication
- User's view of authentication
- FortiGate administrator's view of authentication

What is authentication?

Businesses need to authenticate people who have access to company resources. In the physical world this may be a swipe card to enter the building, or a code to enter a locked door. If a person has this swipe card or code, they have been authenticated as someone allowed in that building or room.

Authentication is the act of confirming the identity of a person or other entity. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit enables controlled network access and applies authentication to users of security policies and VPN clients.

Methods of authentication

FortiGate unit authentication is divided into three basic types: password authentication for people, certificate authentication for hosts or endpoints, and two-factor authentication for additional security beyond just passwords. An exception to this is that FortiGate units in an HA cluster and FortiManager units use password authentication.

Password authentication verifies individual user identities, but access to network resources is based on membership in user groups. For example, a security policy can be configured to permit access only to the members of one or more user groups. Any user who attempts to access the network through that policy is then authenticated through a request for their username and password.

Methods of authentication include:

- Local password authentication
- Server-based password authentication
- Certificate-based authentication
- Two-factor authentication

Local password authentication

The simplest authentication is based on user accounts stored locally on the FortiGate unit. For each account, a username and password is stored. The account also has a disable option so that you can suspend the account without deleting it.

Local user accounts work well for a single-FortiGate installation. If your network has multiple FortiGate units that will use the same accounts, the use of an external authentication server can simplify account configuration and maintenance.

You can create local user accounts in the web-based manager under **User & Device > User > User Definition**. This page is also used to create accounts where an external authentication server stores and verifies the password.

Server-based password authentication

Using external authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server. FortiOS supports the use of LDAP, RADIUS, TACACS+, AD or POP3 servers for authentication.

When you use an external authentication server to authenticate users, the FortiGate unit sends the user's entered credentials to the external server. The password is encrypted. The server's response indicates whether the supplied credentials are valid or not.

You must configure the FortiGate unit to access the external authentication servers that you want to use. The configuration includes the parameters that authenticate the FortiGate unit to the authentication server.

You can use external authentication servers in two ways:

- Create user accounts on the FortiGate unit, but instead of storing each user's password, specify the server used to authenticate that user. As with accounts that store the password locally, you add these users to appropriate user groups.
- Add the authentication server to user groups. Any user who has an account on the server can be authenticated and have the access privileges of the FortiGate user group. Optionally, when an LDAP server is a FortiGate user group member, you can limit access to users who belong to specific groups defined on the LDAP server.

Certificate-based authentication

An RSA X.509 server certificate is a small file issued by a Certificate Authority (CA) that is installed on a computer or FortiGate unit to authenticate itself to other devices on the network. When one party on a network presents the certificate as authentication, the other party can validate that the certificate was issued by the CA. The identification is therefore as trustworthy as the Certificate Authority (CA) that issued the certificate.

To protect against compromised or misused certificates, CAs can revoke any certificate by adding it to a Certificate Revocation List (CRL). Certificate status can also be checked online using Online Certificate Status Protocol (OCSP).

RSA X.509 certificates are based on public-key cryptography, in which there are two keys: the private key and the public key. Data encrypted with the private key can be decrypted only with the public key and vice versa. As the names suggest, the private key is never revealed to anyone and the public key can be freely distributed. Encryption with the recipient's public key creates a message that only the intended recipient can read. Encryption with the sender's private key creates a message whose authenticity is proven because it can be decrypted only with the sender's public key.

Server certificates contain a signature string encrypted with the CA's private key. The CA's public key is contained in a CA root certificate. If the signature string can be decrypted with the CA's public key, the certificate is genuine.

Certificate authorities

A certificate authority can be:

- an organization, such as VeriSign Inc., that provides certificate services
- a software application, such as Microsoft Certificate Services or OpenSSH

For a company web portal or customer-facing SSL VPN, a third-party certificate service has some advantages. The CA certificates are already included in popular web browsers and customers trust the third-party. On the other hand, third-party services have a cost.

For administrators and for employee VPN users, the local CA based on a software application provides the required security at low cost. You can generate and distribute certificates as needed. If an employee leaves the organization, you can simply revoke their certificate.

Certificates for users

FortiGate unit administrators and SSL VPN users can install certificates in their web browsers to authenticate themselves. If the FortiGate unit uses a CA-issued certificate to authenticate itself to the clients, the browser will also need the appropriate CA certificate.

FortiGate IPsec VPN users can install server and CA certificates according to the instructions for their IPsec VPN client software. The FortiClient Endpoint Security application, for example, can import and store the certificates required by VPN connections.

FortiGate units are also compatible with some Public Key Infrastructure systems. For an example of this type of system, see RSA ACE (SecurID) servers on page 458.

Two-factor authentication

A user can be required to provide both something they know (their username and password combination) and something they have (certificate or a random token code). Certificates are installed on the user's computer.

Two-factor authentication is available for PKI users. For more information, see Certificate on page 468.

Another type of two-factor authentication is to use a randomly generated token (multi-digit number) along with the username and password combination. One method is a FortiToken — a one time passcode (OTP) generator that generates a unique code every 60 seconds. Others use email or SMS text messaging to deliver the random token code to the user or administrator.

When one of these methods is configured, the user enters this code at login after the username and password have been verified. The FortiGate unit verifies the token code after as well as the password and username. For more information, see Two-factor authentication on page 467

Types of authentication

FortiOS supports two different types of authentication based on your situation and needs.

Security policy authentication is easily applied to all users logging on to a network, or network service. For example if a group of users on your network such as the accounting department who have access to sensitive data need to access the Internet, it is a good idea to make sure the user is a valid user and not someone trying to send company secrets to the Internet. Security policy authentication can be applied to as many or as few users as needed, and it supports a number of authentication protocols to easily fit with your existing network.

Virtual Private Network (VPN) authentication enables secure communication with hosts located outside the company network, making them part of the company network while the VPN tunnel is operating. Authentication applies to the devices at both ends of the VPN and optionally VPN users can be authenticated as well.

Security policy authentication

Security policies enable traffic to flow between networks. Optionally, the policy can allow access only to specific originating addresses, device types, users or user groups. Where access is controlled by user or user group, users must authenticate by entering valid username and password credentials.

The user's authentication expires if the connection is idle for too long, 5 minutes by default but that can be customized.

Security policies are the mechanism for FSSO, NTLM, certificate based, and RADIUS SSO authentication.

FSSO

Fortinet Single Sign on (FSSO) provides seamless authentication support for Microsoft Windows Active Directory (AD) and Novell eDirectory users in a FortiGate environment.

On a Microsoft Windows or Novell network, users authenticate with the Active Directory or Novell eDirectory at logon. FSSO provides authentication information to the FortiGate unit so that users automatically get access to permitted resources. See Introduction to agent-based FSSO on page 545.

NTLM

The NT LAN Manager (NTLM) protocol is used when the MS Windows Active Directory (AD) domain controller can not be contacted. NTLM is a browser-based method of authentication.

The FSSO software is installed on each AD server and the FortiGate unit is configured to communicate with each FSSO client. When a user successfully logs into their Windows PC (and is authenticated by the AD Server), the FSSO client communicates the user's name, IP address, and group login information to the FortiGate unit. The FortiGate unit sets up a temporary access policy for the user, so when they attempt access through the firewall they do not need to re-authenticate. This model works well in environments where the FSSO client can be installed on all AD servers.

In system configurations where it is not possible to install FSSO clients on all AD servers, the FortiGate unit must be able to query the AD servers to find out if a user has been properly authenticated. This is achieved using the NTLM messaging features of Active Directory and Internet Explorer.

Even when NTLM authentication is used, the user is not asked again for their username and password. Internet Explorer stores the user's credentials and the FortiGate unit uses NTLM messaging to validate them in the Windows AD environment.

Note that if the authentication reaches the timeout period, the NTLM message exchange restarts. For more information on NTLM, see NTLM authentication on page 499 and FSSO NTLM authentication support on page 551.

Certificates

Certificates can be used as part of a policy. All users being authenticated against the policy are required to have the proper certificate. See Certificate-based authentication on page 514

RADIUS SSO

RADIUS Single Sign-On (RSSO) is a remote authentication method that does not require any local users to be configured, and relies on RADIUS Start records to provide the FortiGate unit with authentication information.

That information identifies the user and user group, which is then matched using a security policy. See SSO using RADIUS accounting records on page 589.

FortiGuard Web Filter override authentication

Optionally, users can be allowed the privilege of overriding FortiGuard Web Filtering to view blocked web sites. Depending on the override settings, the override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. As with other FortiGate features, access to FortiGuard overrides is controlled through user groups. Firewall and Directory Services user groups are eligible for the override privilege. For more information about web filtering and overrides, see the UTM chapter of this FortiOS Handbook.

VPN authentication

Authentication involves authenticating the user. In IPsec VPNs authenticating the user is optional, but authentication of the peer device is required.

This section includes:

- Authenticating IPsec VPN peers (devices)
- Authenticating IPsec VPN users
- Authenticating SSL VPN users
- Authenticating PPTP and L2TP VPN users

Authenticating IPsec VPN peers (devices)

A VPN tunnel has one end on a local trusted network, and the other end is at a remote location. The remote peer (device) must be authenticated to be able to trust the VPN tunnel. Without that authentication, it is possible for a malicious hacker to masquerade as a valid VPN tunnel device and gain access to the trusted local network.

The three ways to authenticate VPN peers are with a preshared key, RSA X.509 certificate, or a specific peer ID value.

The simplest way for IPsec VPN peers to authenticate each other is through the use of a preshared key, also called a shared secret. The preshared key is a text string used to encrypt the data exchanges that establish the VPN tunnel. The preshared key must be six or more characters. The VPN tunnel cannot be established if the two peers do not use the same key. The disadvantage of preshared key authentication is that it can be difficult to securely distribute and update the preshared keys.

RSA X.509 certificates are a better way for VPN peers to authenticate each other. Each peer offers a certificate signed by a Certificate Authority (CA) which the other peer can validate with the appropriate CA root certificate. For more information about certificates, see Certificate-based authentication on page 514.

You can supplement either preshared key or certificate authentication by requiring the other peer to provide a specific peer ID value. The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating IPsec VPN users

An IPsec VPN can be configured to accept connections from multiple dynamically addressed peers. You would do this to enable employees to connect to the corporate network while traveling or from home. On a FortiGate unit, you create this configuration by setting the **Remote Gateway** to **Dialup User**.

It is possible to have an IPsec VPN in which remote peer devices authenticate using a common preshared key or a certificate, but there is no attempt to identify the user at the remote peer. To add user authentication, you can do one of the following:

- require a unique preshared key for each peer
- require a unique peer ID for each peer
- require a unique peer certificate for each peer
- require additional user authentication (XAuth)

The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating SSL VPN users

SSL VPN users can be

- user accounts with passwords stored on the FortiGate unit
- user accounts authenticated by an external RADIUS, LDAP or TACACS+ server
- PKI users authenticated by certificate

You need to create a user group for your SSL VPN. Simply create a firewall user group, enable SSL VPN access for the group, and select the web portal the users will access.

SSL VPN access requires an SSL VPN security policy that permits access to members of your user group.

Authenticating PPTP and L2TP VPN users

PPTP and L2TP are older VPN tunneling protocols that do not provide authentication themselves. FortiGate units restrict PPTP and L2TP access to users who belong to one specified user group. Users authenticate themselves to the FortiGate unit by username/password. You can configure PPTP and L2TP VPNs only in the CLI. Before you configure the VPN, create a firewall user group and add to it the users who are permitted to use the VPN. Users are authenticated when they attempt to connect to the VPN. For more information about configuring PPTP or L2TP VPNs, see the FortiGate CLI Reference.

Single Sign-On authentication for users

“Single Sign-On” means that users logged on to a computer network are authenticated for access to network resources through the FortiGate unit without having to enter their username and password again. FortiGate units directly provide Single Sign On capability for:

- Microsoft Windows networks using either Active Directory or NTLM authentication
- Novell networks, using eDirectory

In combination with a FortiAuthenticator unit, the FortiGate unit can provide Single Sign-On capability that integrates multiple external network authentication systems such as Windows Active Directory, Novell e-Directory, RADIUS and LDAP. The FortiAuthenticator unit gathers user logon information from all of these sources and sends it to the FortiGate unit.

Through the SSO feature, the FortiGate unit knows the username, IP address, and external user groups to which the user belongs. When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

For detailed information about SSO, see

- Single Sign-On using a FortiAuthenticator unit on page 533
- Agent-based FSSO on page 545

User's view of authentication

From the user's point of view, they see a request for authentication when they try to access a protected resource, such as an FTP repository of intellectual property or simply access a website on the Internet. The way the request is presented to the user depends on the method of access to that resource.

VPN authentication usually controls remote access to a private network.

Web-based user authentication

Security policies usually control browsing access to an external network that provides connection to the Internet. In this case, the FortiGate unit requests authentication through the web browser.

The user types a username and password and then selects **Continue** or **Login**. If the credentials are incorrect, the authentication screen is redisplayed with blank fields so that the user can try again. When the user enters valid credentials, access is granted to the required resource. In some cases, if a user tries to authenticate several times without success, a message appears, such as: "Too many bad login attempts. Please try again in a few minutes." This indicates the user is locked out for a period of time. This prevents automated brute force password hacking attempts. The administrator can customize these settings if required.

After a defined period of user inactivity (the authentication timeout, defined by the FortiGate administrator), the user's access expires. The default is 5 minutes. To access the resource, the user will have to authenticate again.

VPN client-based authentication

A VPN provides remote clients with access to a private network for a variety of services that include web browsing, email, and file sharing. A client program such as FortiClient negotiates the connection to the VPN and manages the user authentication challenge from the FortiGate unit.

FortiClient can store the username and password for a VPN as part of the configuration for the VPN connection and pass them to the FortiGate unit as needed. Or, FortiClient can request the username and password from the user when the FortiGate unit requests them.

SSL VPN is a form of VPN that can be used with a standard Web browser. There are two modes of SSL VPN operation (supported in NAT/Route mode only):

- web-only mode, for remote clients equipped with a web-browser only
- tunnel mode, for remote computers that run a variety of client and server applications.

After a defined period of user inactivity on the VPN connection (the idle timeout, defined by the FortiGate administrator), the user's access expires. The default is 30 minutes. To access the resource, the user will have to authenticate again.

FortiGate administrator's view of authentication

Authentication is based on user groups. The FortiGate administrator configures authentication for security policies and VPN tunnels by specifying the user groups whose members can use the resource. Some planning is

required to determine how many different user groups need to be created. Individual user accounts can belong to multiple groups, making allocation of user privileges very flexible.

A member of a user group can be:

- a user whose username and password are stored on the FortiGate unit
- a user whose name is stored on the FortiGate unit and whose password is stored on a remote or external authentication server
- a remote or external authentication server with a database that contains the username and password of each person who is permitted access

The general process of setting up authentication is as follows:

1. If remote or external authentication is needed, configure the required servers.
2. Configure local and peer (PKI) user identities. For each local user, you can choose whether the FortiGate unit or a remote authentication server verifies the password. Peer members can be included in user groups for use in security policies.
3. Create user groups.
4. Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server's database can authenticate. You can only configure peer user groups through the CLI.
5. Configure security policies and VPN tunnels that require authenticated access.

For authentication troubleshooting, see the specific chapter for the topic or for general issues see Troubleshooting on page 614.

General authentication settings

Go to **User & Device > Authentication > Settings** to configure authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

- HTTP (can also be set to redirect to HTTPS)
- HTTPS
- FTP
- Telnet

The selections made in the **Protocol Support** list of **Authentication Settings** control which protocols support the authentication challenge. Users must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, it allows the user to authenticate with a customized Local certificate.

When you enable user authentication within a security policy, the security policy user will be challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the unit and the users can also have customized certificates installed on their browsers. Otherwise, users will see a warning message and have to accept a default Fortinet certificate.

Authentication Timeout	Enter a length of time in minutes, from 1 to 1440 (24 hours). Authentication timeout controls how long an authenticated firewall connection can be idle before the user must authenticate again. The default value is 5.
Protocol Support	Select the protocols to challenge during firewall user authentication.
Certificate	If using HTTPS protocol support, select the local certificate to use for authentication. Available only if HTTPS protocol support is selected.
Apply	Select to apply the selections for user authentication settings.

Authentication servers

FortiGate units support the use of external authentication servers. An authentication server can provide password checking for selected FortiGate users or it can be added as a member of a FortiGate user group.

If you are going to use authentication servers, you must configure the servers before you configure FortiGate users or user groups that require them.

Mac OS and iOS devices, including iPhones and iPads, can perform user authentication with FortiOS units using RADIUS servers, but not with LDAP or TACACS+ servers.

This section includes the following topics:

- FortiAuthenticator servers
- RADIUS servers
- LDAP servers
- TACACS+ servers
- POP3 servers
- SSO servers
- RSA ACE (SecurID) servers

FortiAuthenticator servers

FortiAuthenticator is an Authentication, Authorization, and Accounting (AAA) server, that includes a RADIUS server, an LDAP server, and can replace the FSSO Collector Agent on a Windows AD network. Multiple FortiGate units can use a single FortiAuthenticator for FSSO, remote authentication, and FortiToken management.

For more information, see the FortiAuthenticator Administration Guide.

RADIUS servers

Remote Authentication and Dial-in User Service (RADIUS) is a broadly supported client-server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS clients are built into gateways that allow access to networks such as Virtual Private Network servers, Network Access Servers (NAS), as well as network switches and firewalls that use authentication. FortiGate units fall into the last category.

RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to authenticate users before allowing them access to the network, to authorize access to resources by appropriate users, and to account or bill for those resources that are used. RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting), and listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

You must configure the RADIUS server to accept the FortiGate unit as a client. FortiGate units use the authentication and accounting functions of the RADIUS server.

FortiOS does not accept all characters from auto generated keys from MS Windows 2008. These keys are very long and as a result RADIUS authentication will not work. Maximum key length for MS Windows 2008 is 128 bytes. In older versions of FSAE, it was 40 bytes.

Microsoft RADIUS servers

Microsoft Windows Server 2000, 2003, and 2008 have RADIUS support built-in. Microsoft specific RADIUS features are defined in RFC 2548. The Microsoft RADIUS implementation can use Active Directory for user credentials.

For details on Microsoft RADIUS server configurations, refer to Microsoft documentation.

RADIUS user database

The RADIUS user database is commonly an SQL or LDAP database, but can also be any combination of:

- usernames and passwords defined in a configuration file
- user account names and passwords configured on the computer where the RADIUS server is installed.

If users are members of multiple RADIUS groups, then the user group authentication timeout value does not apply. See Membership in multiple groups on page 480.

RADIUS authentication with a FortiGate unit

To use RADIUS authentication with a FortiGate unit

- configure one or more RADIUS servers on the FortiGate unit
- assign users to a RADIUS server

When a configured user attempts to access the network, the FortiGate unit will forward the authentication request to the RADIUS server which will match the username and password remotely. Once authenticated the RADIUS server passes the authorization granted message to the FortiGate unit which grants the user permission to access the network.

The RADIUS server uses a “shared secret” key along with MD5 hashing to encrypt information passed between RADIUS servers and clients, including the FortiGate unit. Typically only user credentials are encrypted. Additional security can be configured through IPsec tunnels by placing the RADIUS server behind another VPN gateway.

RADIUS attribute value pairs

RADIUS packets include a set of attribute value pairs (AVP) to identify information about the user, their location and other information. The FortiGate unit sends the following RADIUS attributes.

FortiOS supported RADIUS attributes

RADIUS Attribute	Name	Description	AVP type
1	Acct-Session-ID	Unique number assigned to each start and stop record to make it easy to match them, and to eliminate duplicate records.	44
2	Username	Name of the user being authenticated	1
3	NAS-Identifier	Identifier or IP address of the Network Access Server (NAS) that is requesting authentication. In this case, the NAS is the FortiGate unit.	32
4	Framed-IP-Address	Address to be configured for the user.	8
5	Fortinet-VSA	See Vendor-specific attributes on page 443	26
6	Acct-Input-Octets	Number of octets received from the port over the course of this service being provided. Used to charge the user for the amount of traffic they used.	42
7	Acct-Output-Octets	Number of octets sent to the port while delivering this service. Used to charge the user for the amount of traffic they used.	43

The following table describes the supported authentication events and the RADIUS attributes that are sent in the RADIUS accounting message.

RADIUS attributes sent in RADIUS accounting message

	RADIUS Attributes						
Authentication Method	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Web	X	X	X		X		
XAuth of IPsec (without DHCP)	X	X	X		X		
XAuth of IPsec (with DHCP)	X	X	X	X	X		
PPTP/L2TP (in PPP)	X	X	X	X	X	X	X
SSL-VPN	X	X	X	X	X		

Vendor-specific attributes

Vendor specific attributes (VSA) are the method RADIUS servers and client companies use to extend the basic functionality of RADIUS. Some major vendors, such as Microsoft, have published their VSAs, however many do not.

In order to support vendor-specific attributes (VSA), the RADIUS server requires a dictionary to define which VSAs to support. This dictionary is typically supplied by the client or server vendor.

The Fortinet RADIUS vendor ID is 12356.

The FortiGate unit RADIUS VSA dictionary is supplied by Fortinet and is available through the Fortinet Knowledge Base (http://kb.forticare.com) or through Technical Support. Fortinet's dictionary for FortiOS 4.0 and up is configured this way:

```
##
Fortinet's VSA's
#
VENDOR fortinet 12356
BEGIN-VENDOR fortinet
ATTRIBUTE Fortinet-Group-Name   1   string
ATTRIBUTE Fortinet-Client-IP-Address   2   ipaddr
ATTRIBUTE Fortinet-Vdom-Name   3   string
ATTRIBUTE Fortinet-Client-IPv6-Address   4   octets
ATTRIBUTE Fortinet-Interface-Name   5   string
ATTRIBUTE Fortinet-Access-Profile   6   string
#
# Integer Translations
#
END-VENDOR Fortinet
```

Note that using the Fortinet-Vdom-Name, users can be tied to a specific VDOM on the FortiGate unit. See the documentation provided with your RADIUS server for configuration details.

Role Based Access Control

In Role Based Access Control (RBAC), network administrators and users have varying levels of access to network resources based on their role, and that role's requirement for access specific resources. For example, a junior accountant does not require access to the sales presentations, or network user account information.

There are three main parts to RBAC: role assignment, role authorization, and transaction authorization. Role assignment is accomplished when someone in an organization is assigned a specific role by a manager or HR. Role authorization is accomplished when a network administrator creates that user's RADIUS account and assigns them to the required groups for that role. Transaction authorization occurs when that user logs on and authenticates before performing a task.

RBAC is enforced when FortiOS network users are remotely authenticated via a RADIUS server. For users to authenticate, a security policy must be matched. That policy only matches a specific group of users. If VDOMs are enabled, the matched group will be limited to a specific VDOM. Using this method network administrators can separate users into groups that match resources, protocols, or VDOMs. It is even possible to limit users to specific FortiGate units if the RADIUS servers serve multiple FortiOS units.

For more information on security policies, see Authentication in security policies on page 492.

Configuring the FortiGate unit to use a RADIUS server

The information you need to configure the FortiGate unit to use a RADIUS server includes

- the RADIUS server's domain name or IP address
- the RADIUS server's shared secret key.

You can optionally specify the NAS IP or Called Station ID. When configuring the FortiGate to use a RADIUS server, the FortiGate is a Network Access Server (NAS). If the FortiGate interface has multiple IP addresses, or you want the RADIUS requests to come from a different address you can specify it here. Called Station ID applies to carrier networks. However, if the NAS IP is not included in the RADIUS configuration, the IP of the FortiGate unit interface that communicates with the RADIUS server is used instead.

A maximum of 10 remote RADIUS servers can be configured on the FortiGate unit. One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 464.

On the FortiGate unit, the default port for RADIUS traffic is 1812. Some RADIUS servers use port 1645. If this is the case with your server, you can either:

- Re-configure the RADIUS server to use port 1812. See your RADIUS server documentation for more information on this procedure.

or

- Change the FortiGate unit default RADIUS port to 1645 using the CLI:

```
config system global
   set radius-port 1645
end
```

One wildcard admin account can be added to the FortiGate unit when using RADIUS authentication. This uses the wildcard character to allow multiple admin accounts on RADIUS to use a single account on the FortiGate unit. See Example — wildcard admin accounts - CLI on page 451.

To configure the FortiGate unit for RADIUS authentication - web-based manager:

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information and select **OK**.

Name	A name to identify the RADIUS server on the FortiGate unit.
Primary Server Name/IP	Enter the domain name (such as fgt.exmaple.com) or the IP address of the RADIUS server.
Primary Server Secret	Enter the server secret key, such as radiusSecret. This can be a maximum of 16 characters long. This must match the secret on the RADIUS primary server.
Secondary Server Name/IP	Optionally enter the domain name (such as fgt.exmaple.com) or the IP address of the secondary RADIUS server.

Secondary Server Secret	Optionally, enter the secondary server secret key, such as radiusSecret2. This can be a maximum of 16 characters long. This must match the secret on the RADIUS secondary server.
Authentication Scheme	If you know the RADIUS server uses a specific authentication protocol, select it from the list. Otherwise select **Use Default Authentication Scheme**. The Default option will usually work.
NAS IP/ Called Station ID	Enter the IP address to be used as an attribute in RADIUS access requests. **NAS-IP-Address** is RADIUS setting or IP address of FortiGate interface used to talk to RADIUS server, if not configured. **Called Station ID** is same value as NAS-IP Address but in text format.
Include in every User Group	When enabled this RADIUS server will automatically be included in all user groups. This is useful if all users will be authenticating with the remote RADIUS server.

For MAC OS and iOS devices to authenticate, you must use MS-CHAP-v2 authentication. In the CLI, the command is `set auth-type ms_chap_v2`.

3. Select **OK**.

To configure the FortiGate unit for RADIUS authentication - CLI example:

```
config user radius
   edit ourRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret radiusSecret
   end
```

For more information about RADIUS server options, refer to the FortiGate CLI Reference.

Troubleshooting RADIUS

To test the connection to the RADIUS server use the following command:

```
diagnose test authserver radius-direct <server_name or IP> <port number> <secret>
```

For the port number, enter `-1` to use the default port. Otherwise enter the port number to check.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

The scale of LDAP servers range from big public servers such as BigFoot and Infospace, to large organizational servers at universities and corporations, to small LDAP servers for workgroups that may be using OpenLDAP. This document focuses on the institutional and workgroup applications of LDAP.

This section includes:

- Components and topology
- LDAP directory organization
- Configuring the FortiGate unit to use an LDAP server
- Example — wildcard admin accounts - CLI
- Example of LDAP to allow Dial-in through member-attribute - CLI
- Troubleshooting LDAP

Components and topology

LDAP organization starts with directories. A directory is a set of objects with similar attributes organized in a logical and hierarchical way. Generally, an LDAP directory tree reflects geographic and organizational boundaries, with the Domain name system (DNS) names to structure the top level of the hierarchy. The common name identifier for most LDAP servers is `cn`, however some servers use other common name identifiers such as `uid`.

When LDAP is configured and a user is required to authenticate the general steps are:

1. The FortiGate unit contacts the LDAP server for authentication.
2. To authenticate with the FortiGate unit, the user enters a username and password.
3. The FortiGate unit sends this username and password to the LDAP server.
4. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit.
5. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

Binding

Binding is the step where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on that user's permissions.

The FortiGate unit can be configured to use one of three types of binding:

- anonymous - bind using anonymous user search
- regular - bind using username/password and then search
- simple - bind using a simple password authentication without a search

You can use simple authentication if the user records all fall under one domain name (`dn`). If the users are under more than one `dn`, use the anonymous or regular type, which can search the entire LDAP database for the required username.

If your LDAP server requires authentication to perform searches, use the regular type and provide values for username and password.

Supported versions

The FortiGate unit supports LDAP protocol functionality defined in RFC 2251: Lightweight Directory Access Protocol v3, for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers

compliant with LDAP v3, including FortiAuthenticator. In addition, FortiGate LDAP supports LDAP over SSL/TLS, which can be configured only in the CLI.

FortiGate LDAP does not support proprietary functionality, such as notification of password expiration, which is available from some LDAP servers. FortiGate LDAP does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

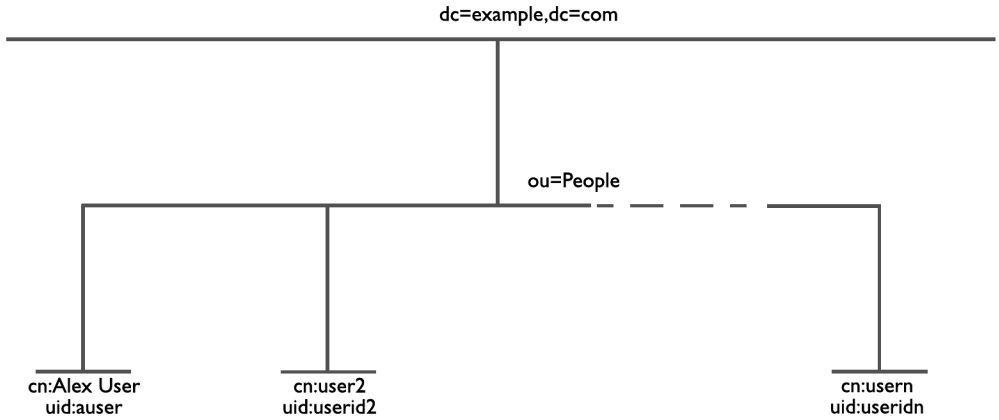
LDAP directory organization

To configure your FortiGate unit to work with an LDAP server, you need to understand the organization of the information on the server.

The top of the hierarchy is the organization itself. Usually this is defined as Domain Component (DC), a DNS domain. If the name contains a dot, such as `example.com`, it is written as two parts separated by a comma: `dc=example,dc=com`.

In this example, Common Name (CN) identifiers reside at the Organization Unit (OU) level, just below DC. The Distinguished Name (DN) is ou=People,dc=example,dc=com.

LDAP object hierarchy



In addition to the DN, the FortiGate unit needs an identifier for the individual person. Although the FortiGate unit GUI calls this the Common Name (CN), the identifier you use is not necessarily CN. On some servers, CN is the full name of a person. It might be more convenient to use the same identifier used on the local computer network. In this example, User ID (UID) is used.

Locating your identifier in the hierarchy

You need to determine the levels of the hierarchy from the top to the level that contain the identifier you want to use. This defines the DN that the FortiGate unit uses to search the LDAP database. Frequently used distinguished name elements include:

- uid (user identification)
- pw (password)
- cn (common name)
- ou (organizational unit)
- o (organization)
- c (country)

One way to test this is with a text-based LDAP client program. For example, OpenLDAP includes a client, `ldapsearch`, that you can use for this purpose.

Enter the following at the command line:

```
ldapsearch -x '(objectclass=*)'
```

The output is lengthy, but the information you need is in the first few lines:

```
version: 2
#
# filter: (objectclass=*)
# requesting: ALL

dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain

dn: ou=People,dc=example,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
...
dn: uid=tbrown,ou=People,dc=example,dc=com
uid: tbrown
cn: Tom Brown
```

In the output above, you can see `tbrown` (uid) and `Tom Brown`(cn). Also note the dn is `ou=People, dc=example, dc=com`.

Configuring the FortiGate unit to use an LDAP server

After you determine the common name and distinguished name identifiers and the domain name or IP address of the LDAP server, you can configure the server on the FortiGate unit. The maximum number of remote LDAP servers that can be configured is 10.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 464.

To configure the FortiGate unit for LDAP authentication - web-based manager:

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter a **Name** for the LDAP server.
3. In **Server Name/IP** enter the server's FQDN or IP address.
4. If necessary, change the **Server Port** number. The default is port 389.
5. Enter the **Common Name Identifier** (20 characters maximum).
   `cn` is the default, and is used by most LDAP servers.
6. In the **Distinguished Name** field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   If you don't know the distinguished name, leave the field blank and select the Query icon to the right of the field. See Using the Query icon on page 450.
7. In the **Distinguished Name** field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   If you don't know the distinguished name, leave the field blank and select the Query icon to the right of the field. See Using the Query icon on page 450.
8. In **Bind Type**, select **Regular**.
9. In **User DN**, enter the LDAP administrator's distinguished name.
10. In **Password**, enter the LDAP administrator's password.
11. Select **OK**.

To verify your Distinguished Name field is correct, you can select the **Test** button. If your DN field entry is valid, you will see the part of the LDAP database it defines. If your DN field entry is not valid, it will display an error message and return no information.

For detailed information about configuration options for LDAP servers, see the Online Help on your FortiGate unit or the FortiGate CLI Reference.

To configure the FortiGate unit for LDAP authentication - CLI example:

```
config user ldap
   edit ourLDAPsrv
      set server 10.11.101.160
      set cnid cn
      set dn cn=users,dc=office,dc=example,dc=com
      set type regular
      set username cn=administrator,cn=users,dc=office,dc=example,dc=com
      set password w5AiGVMLkgyPQ
      set password-expiry-warning enable
      set password-renewal enable
   end
```

password-expiry-warning and password-renewal

In SSLVPN, when an LDAP user is connecting to the LDAP server it is possible for them to receive any pending password expiry or renewal warnings. When the password renewal or expiry warning exists, SSLVPN users will see a prompt allowing them to change their password.

`password-expiry-warning` allows FortiOS to detect from the LDAP server when a password is expiring or has expired using server controls or error codes.

`password-renewal` allows FortiOS to perform the online LDAP password renewal operations the LDAP server expects.

On an OpenLDAP server, when a user attempts to logon with an expired password they are allowed to logon but only to change their password.

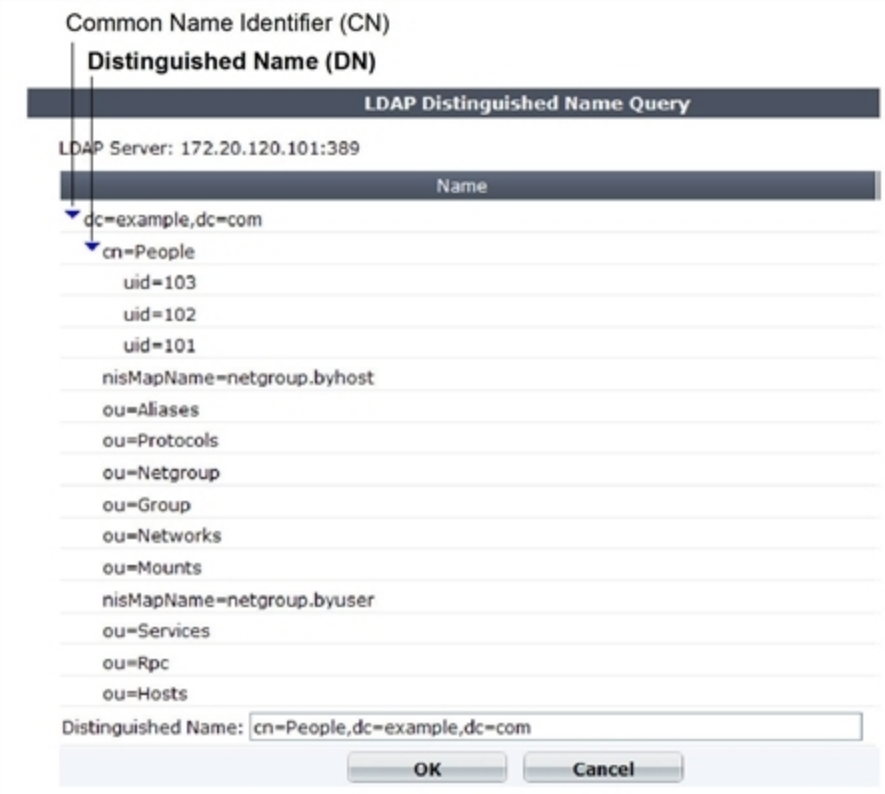
When changing passwords on a Windows AD system, the connection must be SSL-protected.

Using the Query icon

The LDAP Distinguished Name Query list displays the LDAP directory tree for the LDAP server connected to the FortiGate unit. This helps you to determine the appropriate entry for the DN field. To see the distinguished name associated with the Common Name identifier, select the Expand icon next to the CN identifier. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration.

To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.

LDAP server Distinguished Name Query tree



Example — wildcard admin accounts - CLI

A wildcard admin account is an administrator account with the wildcard option enabled. This option allows multiple different remote administration accounts to match one local administration account, avoiding the need to set up individual admin accounts on the FortiGate unit. Instead multiple LDAP admin accounts will all be able to use one FortiGate admin account.

The initial benefit of wildcard admin accounts is fast configuration of the FortiGate unit's administration account to work with your LDAP network. The many to one ratio saves on effort, and potential errors.

The ongoing benefit is that as long as the users on the LDAP system belong to that group, and the test admin user settings don't change on the FortiGate unit, no other work is required. This point is important as it can help avoid system updates or changes that would otherwise require changes to the LDAP administrator account configuration. Even if a user is added to or removed from the LDAP group, no changes are required on the FortiGate unit.

Two potential issues with wildcard admin accounts are that multiple users may be logged on to the same account at the same time. This becomes an issue if they are changing the same information at the same time. The other potential issue is that security is reduced because multiple people have login access for the same account. If each user was assigned their own account, a hijacking of one account would not affect the other users.

Note that wildcard admin configuration also applies to RADIUS. When configuring for RADIUS, configure the RADIUS server, and RADIUS user group instead of LDAP. When using web-based management, wildcard admin is the only type of remote administrator account that does not require you to enter a password on account

creation. That password is normally used when the remote authentication server is unavailable during authentication.

In this example, default values are used where possible. If a specific value is not mentioned, it is set to its default value.

Configuring the LDAP server

The important parts of this configuration are the username and group lines. The username is the domain administrator account. The group binding allows only the group with the name `GRP` to access.

The `dn` used here is as an example only. On your network use your own domain name.

To configure LDAP server - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=example,DC=com,DC=au"
      set type regular
      set username "CN=Administrator,CN=Users,DC=example,DC=COM”
      set password *
      set group-member-check group-object
      set group-object-filter (&
          (objectcategory=group)member="CN=GRP,OU=training,DC=example,DC=COM"))
   next
end
```

To configure the user group and add the LDAP server - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
         config match
            edit 1
               set server-name "ldap_server"
               set group-name "CN=GRP,OU=training,DC=example,DC=COM"
            next
         end
      next
   end
```

Configuring the admin account

The wildcard part of this example is only available in the CLI for admin configuration. When enabled, this allows all LDAP group members to login to the FortiGate unit without the need to create a separate admin account for each user. In effect the members of that group will each be able to login as “test”.

To configure the admin account - CLI:

```
config system admin
```

```
    edit "test"
      set remote-auth enable
      set accprofile "super_admin"
      set wildcard enable
      set remote-group "ldap_grp"
    next
end
```

For troubleshooting, test that the admin account is operational, and see Troubleshooting LDAP on page 454.

Example of LDAP to allow Dial-in through member-attribute - CLI

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to setup a VPN connection simply based on an attribute that is set to TRUE, instead of based on being part of a specific group.

In AD, the “Allow Dial-In” property is activated in the user properties, and this sets the `msNPAllowDialin` attribute to “TRUE”.

This same procedure can be used for other member attributes, as your system requires.

Configuring LDAP member-attribute settings

To accomplish this with a FortiGate unit, the member attribute must be set. Setting member attributes can only be accomplished through the CLI using the `member-attr` keyword - the option is not available through the web-based manager.

Before configuring the FortiGate unit, the AD server must be configured and have the `msNPAllowDialin` attribute set to “TRUE” for the users in question. If not, those users will not be able to properly authenticate.

The dn used here is as an example only. On your network use your own domain name.

To configure user LDAP member-attribute settings - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=fortinet,DC=com,DC=au"
      set type regular
      set username "fortigate@example.com"
      set password ******
      set member-attr "msNPAllowDialin"
   next
end
```

Configuring LDAP group settings

A user group that will use LDAP must be configured. This example adds the member `ldap` to the group which is the LDAP server name that was configured earlier.

To configure LDAP group settings - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
      config match
```

```
        edit 1
           set server-name "ldap"
           set group-name "TRUE"
        next
     end
  end
```

Once these settings are in place, users can authenticate.

Troubleshooting LDAP

The examples in this section use the values from the previous example.

LDAP user test

A quick way to see if the LDAP configuration is correct is to run a diagnose CLI command with LDAP user information. The following command tests with a user called `netAdmin` and a password of `fortinet`. If the configuration is correct the test will be successful.

```
FGT# diag test authserver ldap ldap_server netAdmin fortinet
```

`'ldap_server' is not a valid ldap server name` — an LDAP server by that name has not been configured on the FortiGate unit, check your spelling.

`authenticate 'netAdmin' against 'ldap_server' failed!` — the user `netAdmin` does not exist on `ldap_server`, check your spelling of both the user and sever and ensure the user has been configured on the FortiGate unit.

LDAP authentication debugging

For a more in-depth test, you can use a `diag debug` command. The sample output from a shows more information about the authentication process that may prove useful if there are any problems.

Ensure the “Allow Dial-in” attribute is still set to “TRUE” and run the following CLI command. `fnbamd` is the Fortinet non-blocking authentication daemon.

```
FGT# diag debug enable
FGT# diag debug reset
FGT# diag debug application fnbamd -1
FGT# diag debug enable
```

The output will look similar to:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the “Allow Dial-in” attribute is not set but it is expected, the last line of the above output will instead be:

```
fnbamd_auth_poll_ldap-Failed group matching
```

TACACS+ servers

When users connect to their corporate network remotely, they do so through a remote access server. As remote access technology has evolved, the need for security when accessing networks has become increasingly important. This need can be filled using a Terminal Access Controller Access-Control System (TACACS+) server.

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a username and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies, and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP protocol.

There are several different authentication protocols that TACACS+ can use during the authentication process:

Authentication protocols

Protocol	Definition
ASCII	Machine-independent technique that uses representations of English characters. Requires user to type a username and password that are sent in clear text (unencrypted) and matched with an entry in the user database stored in ASCII format.
PAP	Password Authentication Protocol (PAP) Used to authenticate PPP connections. Transmits passwords and other user information in clear text.
CHAP	Challenge-Handshake Authentication Protocol (CHAP) Provides the same functionality as PAP, but is more secure as it does not send the password and other user information over the network to the security server.
MS-CHAP	MicroSoft Challenge-Handshake Authentication Protocol v1 (MSCHAP) Microsoft-specific version of CHAP.
default	The default protocol configuration, Auto, uses PAP, MS-CHAP, and CHAP, in that order.

Configuring a TACACS+ server on the FortiGate unit

A maximum of 10 remote TACACS+ servers can be configured for authentication.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 464.

The TACACS+ page in the web-based manager is not available until a TACACS+ server has been configured in the CLI. For more information see the CLI Reference.

To configure the FortiGate unit for TACACS+ authentication - web-based manager:

1. Go to **User & Device > Authentication > TACACS+ Servers** and select **Create New**.
2. Enter the following information, and select **OK**.

Name	Enter the name of the TACACS+ server.
Server Name/IP	Enter the server domain name or IP address of the TACACS+ server.
Server Key	Enter the key to access the TACACS+ server.
Authentication Type	Select the authentication type to use for the TACACS+ server. **Auto** tries PAP, MSCHAP, and CHAP (in that order).

To configure the FortiGate unit for TACACS+ authentication - CLI:

```
config user tacacs+
   edit tacacs1
      set authen-type auto
      set key abcdef
      set port 49
      set server 192.168.0.101
   end
```

POP3 servers

FortiOS can authenticate users who have accounts on POP3 or POP3s email servers. POP3 authentication can be configured only in the CLI.

To configure the FortiGate unit for POP3 authentication:

```
config user pop3
   edit pop3_server1
      set server pop3.fortinet.com
      set secure starttls
      set port 110
   end
```

To configure a POP3 user group:

```
config user group
   edit pop3_grp
      set member pop3_server1
   end
```

A user group can list up to six POP3 servers as members.

SSO servers

Novell and Microsoft Windows networks provide user authentication based on directory services: eDirectory for Novell, Active Directory for Windows. Users can log on at any computer in the domain and have access to resources as defined in their user account. The Fortinet Single Sign On (FSSO) agent enables FortiGate units to authenticate these network users for security policy or VPN access without asking them again for their username and password.

When a user logs in to the Windows or Novell domain, the FSSO agent sends to the FortiGate unit the user's IP address and the names of the user groups to which the user belongs. The FortiGate unit uses this information to

maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the FortiGate unit does not perform authentication. It recognizes group members by their IP address.

In the FortiOS FSSO configuration, you specify the server where the FSSO Collector agent is installed. The Collector agent retrieves the names of the Novell or Active Directory user groups from the domain controllers on the domains, and then the FortiGate unit gets them from the Collector agent. You cannot use these groups directly. You must define FSSO type user groups on your FortiGate unit and then add the Novell or Active Directory user groups to them. The FSSO user groups that you created are used in security policies and VPN configurations to provide access to different services and resources.

FortiAuthenticator servers can replace the Collector agent when FSSO is using polling mode. The benefits of this is that FortiAuthenticator is a stand-alone server that has the necessary FSSO software pre-installed. For more information, see the FortiAuthenticator Administration Guide.

Single Sign-on Agent configuration settings

The following are SSO configuration settings in **User & Device > Authentication > Single Sign-On**.

SSO Server List

Lists all the collector agents' lists that you have configured. On this page, you can create, edit or delete FSSO agents. There are different types of FSSO agents, each with its own settings.

Note: You can create a redundant configuration on your unit if you install a collector agent on two or more domain controllers. If the current (or first) collector agent fails, the Fortinet unit switches to the next one in its list of up to five collector agents.

Create New	Creates a new agent. When you select **Create New**, you are automatically redirected to the New page.
Edit	Modifies the settings for the selected SSO server. To remove multiple entries from the list, for each servers you want removed, select the check box and then select **Delete**. To remove all agents from the list, on the FSSO Agent page, select the check box at the top of the check box column and then select **Delete**.
Delete	Removes an agent from the list on the page.

Settings when Type is Poll Active Directory Server	
Server IP/Name	The IP address of the domain controller (DC).
User	The user ID used to access the domain controller.
Password	Enter the password for the account used to access the DC.
LDAP Server	Select the check box and select an LDAP server to access the Directory Service.
Enable Polling	Enable to allow the FortiGate unit to poll this DC.
Users/Groups	A list of user and user group names retrieved from the DC.

Settings when Type is Fortinet Single Sign On Agent	
Name	Enter a name for the SSO server.
Primary Agent IP/Name **Secondary Agent IP/Name**	Enter the IP address or name of the Directory Service server where this SSO agent is installed. The maximum number of characters is 63.
Password	Enter the password for the collector agent. This is required only if you configured your Fortinet Single Sign On Agent collector agent to require authenticated access.
LDAP Server	Select the check box and select an LDAP server to access the Directory Service.
More FSSO agents	Select to add up to three additional SSO agents.
Users/Groups	A list of user and user group names retrieved from the server.

Settings when Type is RADIUS Single Sign On Agent	
Use RADIUS Shared Secret	Enable
Shared Secret	Enter the RADIUS server shared secret.
Send RADIUS Responses	Enable.

RSA ACE (SecurID) servers

SecurID is a two-factor system that uses one-time password (OTP) authentication. It is produced by the company RSA. This system includes portable tokens carried by users, an RSA ACE/Server, and an Agent Host. In our configuration, the FortiGate unit is the Agent Host.

Components

When using SecurID, users carry a small device or “token” that generates and displays a pseudo-random password. According to RSA, each SecurID authenticator token has a unique 64-bit symmetric key that is combined with a powerful algorithm to generate a new code every 60 seconds. The token is time-synchronized with the SecurID RSA ACE/Server.

The RSA ACE/Server is the management component of the SecurID system. It stores and validates the information about the SecurID tokens allowed on your network. Alternately the server could be an RSA SecurID 130 Appliance.

The Agent Host is the server on your network, in this case it is the FortiGate unit, that intercepts user logon attempts. The Agent Host gathers the user ID and password entered from their SecurID token, and sends that

information to the RSA ACE/Server to be validated. If valid, a reply comes back indicating it is a valid logon and the FortiGate unit allows the user access to the network resources specified in the associated security policy.

Configuring the SecurID system

To use SecurID with a FortiGate unit, you need:

- to configure the RSA server and the RADIUS server to work with each other (see RSA server documentation)
- to configure the RSA SecurID 130 Appliance
  or
- to configure the FortiGate unit as an Agent Host on the RSA ACE/Server
- to configure the FortiGate unit to use the RADIUS server
- to create a SecurID user group
- to configure a security policy with SecurID authentication

The following instructions are based on RSA ACE/Server version 5.1, or RSA SecurID 130 Appliance, and assume that you have successfully completed all the external RSA and RADIUS server configuration steps listed above.

For this example, the RSA server is on the internal network, with an IP address of 192.128.100.100. The FortiGate unit internal interface address is 192.168.100.3, RADIUS shared secret is fortinet123, RADIUS server is at IP address 192.168.100.102.

To configure the RSA SecurID 130 Appliance

1. Go to the IMS Console for SecurID and logon.
2. Go to **RADIUS > RADIUS Clients**, and select **Add New.**
3. Enter the following information to configure your FortiGate as a SecurID Client, and select Save.

RADIUS Client Basics	
Client Name	FortiGate
Associated RSA Agent	FortiGate

RADIUS Client Settings	
IP Address	192.168.100.3 The IP address of the FortiGate unit internal interface.
Make / Model	Select Standard Radius
Shared Secret	fortinet123 The RADIUS shared secret.
Accounting	Leave unselected
Client Status	Leave unselected

To configure the FortiGate unit as an Agent Host on the RSA ACE/Server

1. On the RSA ACE/Server computer, go to **Start > Programs > RSA ACE/Server**, and then **Database Administration - Host Mode**.
2. On the **Agent Host** menu, select **Add Agent Host**.
3. Enter and save the following information.

Name	FortiGate
Network Address	192.168.100.3 The IP address of the FortiGate unit.
Secondary Nodes	Optionally enter other IP addresses that resolve to the FortiGate unit.

If needed, refer to the RSA ACE/Server documentation for more information.

To configure the FortiGate unit to use the RADIUS server

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information, and select **OK**.

Name	RSA
Primary Server IP/Name	192.168.100.102 Optionally select Test to ensure the IP address is correct and the FortiGate can contact the RADIUS server.
Primary Server Secret	fortinet123
Authentication Scheme	Select **Use Default Authentication Scheme**.

To create a SecurID user group

1. Go to **User & Device > User > User Groups**, and select **Create New**.
2. Enter the following information.

Name	RSA_group
Type	Firewall

3. In **Remote Groups**, select **Add**, then select the RSA server.
4. Select **OK**.

To create a SecurID user:

1. Go to **User & Device > User > User Definition**, and select **Create New**.
2. Use the wizard to enter the following information, and then select **Create**.

User Type	Remote RADIUS User
User Name	wloman
RADIUS Server	RSA
Contact Info	(optional) Enter Email or SMS information
User Group	RSA_group

To test this configuration, on your FortiGate unit use the CLI command:

```
diagnose test authserver radius RSA auto wloman 111111111
```

The series of 1s is the one time password that your RSA SecurID token generates and you enter.

Using the SecurID user group for authentication

You can use the SecurID user group in several FortiOS features that authenticate by user group including

- Security policy
- IPsec VPN XAuth
- PPTP VPN
- SSL VPN

The following sections assume the SecurID user group is called `securIDgrp` and has already been configured. Unless otherwise states, default values are used.

Security policy

To use SecurID in a security policy, you must include the SecurID user group in a security policy. This procedure will create a security policy that allows HTTP, FTP, and POP3 traffic from the `internal` interface to `wan1`. If these interfaces are not available on your FortiGate unit, substitute other similar interfaces.

To configure a security policy with SecurID authentication

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Enter:

Incoming Interface	internal
Source Address	all
Source User(s)	securIDgrp
Outgoing Interface	wan1
Destination Address	all
Schedule	always

Services	HTTP, FTP, POP3
Action	ACCEPT
NAT	On
Shared Shaper	On, if you want to either limit traffic or guarantee minimum bandwidth for traffic that uses the SecurID security policy. Use the default shaper **guarantee-100kbps**.
Log Allowed Traffic	On, if you want to generate usage reports on traffic authenticated with this policy.

4. Select **OK**.
   The SecurID security policy is configured.

For more detail on configuring security policies, see the FortiOS Handbook FortiGate Fundamentals guide.

IPsec VPN XAuth

Extended Authentication (XAuth) increases security by requiring user authentication in addition to the preshared key.

When creating an IPsec VPN using the wizard (**VPN > IPsec > Wizard**), select the SecurID **User Group** on the Authentication page. Members of the SecurID group are required to enter their SecureID code to authenticate.

For more on XAuth, see Configuring XAuth authentication on page 502

PPTP VPN

PPTP VPN is configured in the CLI. In the PPTP configuration (`config vpn pptp`), set `usrgrp` to the SecurID user group.

SSL VPN

You need to map the SecurID user group to the portal that will serve SecurID users and include the SecurID user group in the **Source User(s)** field in the security policy.

To map the SecurID group to an SSL VPN portal:

1. Go to **VPN > SSL > Settings**.
2. In **Authentication/Portal Mapping**, select **Create New**.
3. Enter

Users/Groups	securIDgrp
Portal	Choose the portal.

4. Select **OK**.

Users and user groups

FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user's access to network resources. The members of user groups are user accounts, of which there are several types. Local users and peer users are defined on the FortiGate unit. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and then how to configure user groups. For information about configuration of authentication servers see Authentication servers on page 440.

This section contains the following topics:

- Users
- User groups

Users

A user is a user account consisting of username, password, and in some cases other information, configured on the FortiGate unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. There are several different types of user accounts with slightly different methods of authentication:

User type	Authentication
Local user	The username and password must match a user account stored on the FortiGate unit. Authentication by FortiGate security policy.
Remote user	The username must match a user account stored on the FortiGate unit and the username and password must match a user account stored on the remote authentication server. FortiOS supports LDAP, RADIUS, and TACACS+ servers.
Authentication server user	A FortiGate user group can include user accounts or groups that exist on a remote authentication server.
FSSO user	With Fortinet Single Sign On (FSSO), users on a Microsoft Windows or Novell network can use their network authentication to access resources through the FortiGate unit. Access is controlled through FSSO user groups which contain Windows or Novell user groups as their members.
PKI or Peer user	A Public Key Infrastructure (PKI) or peer user is a digital certificate holder who authenticates using a client certificate. No password is required, unless two-factor authentication is enabled.
IM Users	IM users are not authenticated. The FortiGate unit can allow or block each IM user name from accessing the IM protocols. A global policy for each IM protocol governs access to these protocols by unknown users.
Guest Users	Guest user accounts are temporary. The account expires after a selected period of time.

This section includes:

- Local and remote users
- PKI or peer users
- Two-factor authentication
- FortiToken
- Monitoring users

Local and remote users

Local and remote users are defined on the FortiGate unit in **User & Device > User > User Definition**.

Create New	Creates a new user account. When you select **Create New**, you are automatically redirected to the User Creation Wizard.
Edit User	Modifies a user's account settings. When you select **Edit**, you are automatically redirected to the Edit User page.
Delete	Removes a user from the list. Removing the user name removes the authentication configured for the user. The **Delete** icon is not available if the user belongs to a user group. To remove multiple local user accounts from within the list, on the User page, in each of the rows of user accounts you want removed, select the check box and then select **Delete**. To remove all local user accounts from the list, on the User page, select the check box in the check box column and then select **Delete**.
User Name	The user name. For a remote user, this username must be identical to the username on the authentication server.
Type	Local indicates a local user authenticated on the FortiGate unit. For remote users, the type of authentication server is shown: LDAP, RADIUS, or TACACS+.
Two-factor Authentication	Indicates whether two-factor authentication is configured for the user.
Ref.	Displays the number of times this object is referenced by other objects. Select the number to open the Object Usage window and view the list of referring objects. The list is grouped into expandable categories, such as Firewall Policy. Numbers of objects are shown in parentheses. To view more information about the referring object, use the icons: • **View the list page for these objects** – available for object categories. Goes to the page where the object is listed. For example, if the category is User Groups, opens User Groups list. • **Edit this object** – opens the object for editing. • **View the details for this object** – displays current settings for the object.

To create a local or remote user account - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. On the **Choose User Type** page select:

Local User	Select to authenticate this user using a password stored on the FortiGate unit.
Remote RADIUS User **Remote TACACS+ User** **Remote LDAP User**	To authenticate this user using a password stored on an authentication server, select the type of server and then select the server from the list. You can select only a server that has already been added to the FortiGate unit configuration.

3. Select **Next** and provide user authentication information.
   For a local user, enter the **User Name** and **Password**.
   For a remote user, enter the **User Name** and the server name.
4. Select **Next** and enter **Contact Information**.
   If email or SMS is used for two-factor authentication, provide the email address or SMS cell number at which the user will receive token password codes. If a custom SMS service is used, it must already be configured in **System > Config > Advanced >SMS Service**. See FortiToken on page 470.
5. Select **Next**, then on the **Provide Extra Info** page enter

Two-factor Authentication	Select to enable two-factor authentication. Then select the Token (FortiToken or FortiToken Mobile) for this user account. See Associating FortiTokens with accounts on page 474.
User Group	Select the user groups to which this user belongs.

6. Select **Create**.

To create a local user - CLI example:

Locally authenticated user

```
config user local
   edit user1
      set type password
      set passwd ljt_pj2gpepfdw
   end
```

To create a remote user - CLI example:

```
config user local
   edit user2
      set type ldap
      set ldap_server ourLDAPsrv
   end
```

For a RADIUS or TACACS+ user, set `type` to `radius` or `tacacs+`, respectively.

To create a user with FortiToken Mobile two-factor authentication - CLI example:

```
config user local
   edit user5
      set type password
      set passwd ljt_pj2gpepfdw
      set two_factor fortitoken
      set fortitoken 182937197
   end
```

Remote users are configured for FortiToken two-factor authentication similarly.

To create a user with SMS two-factor authentication using FortiGuard messaging Service - CLI example:

```
config user local
   edit user6
      set type password
      set passwd 3ww_pjt68dw
      set two_factor sms
      set sms-server fortiguard
      set sms-phone 1365984521
   end
```

Removing users

Best practices dictate that when a user account is no longer in use, it should be deleted. Removing local and remote users from FortiOS involve the same steps.

If the user account is referenced by any configuration objects, those references must be removed before the user can be deleted. See Removing references to users on page 466.

To remove a user from the FortiOS configuration - web-based manager:

1. Go to **User & Device > User > User Definition**.
2. Select the check box of the user that you want to remove.
3. Select **Delete**.
4. Select **OK**.

To remove a user from the FortiOS configuration - CLI example:

```
config user local
   delete user4444
end
```

Removing references to users

You cannot remove a user that belongs to a user group. Remove the user from the user group first, and then delete the user.

To remove references to a user - web-based manager

1. Go to **User & Device > User > User Definition**.
2. If the number in the far right column for the selected user contains any number other than zero, select it.

3. A more detailed list of object references to this user is displayed. Use its information to find and remove these references to allow you to delete this user.

PKI or peer users

A PKI, or peer user, is a digital certificate holder. A PKI user account on the FortiGate unit contains the information required to determine which CA certificate to use to validate the user's certificate. Peer users can be included in firewall user groups or peer certificate groups used in IPsec VPNs. For more on certificates, see Certificates overview on page 515.

To define a peer user you need:

- a peer username
- the text from the subject field of the user's certificate, or the name of the CA certificate used to validate the user's certificate

Creating a peer user

The peer user can be configured only in the CLI.

To create a peer user for PKI authentication - CLI example:

```
config user peer
   edit peer1
      set subject peer1@mail.example.com
      set ca CA_Cert_1
   end
```

There are other configuration settings that can be added or modified for PKI authentication. For example, you can configure the use of an LDAP server to check access rights for client certificates. For information about the detailed PKI configuration settings, see the FortiGate CLI Reference.

Two-factor authentication

The standard logon requires a username and password. This is one factor authentication—your password is one piece of information you need to know to gain access to the system.

Two factor authentication adds the requirement for another piece of information for your logon. Generally the two factors are something you know (password) and something you have (certificate, token, etc.). This makes it harder for a hacker to steal your logon information. For example if you have a FortiToken device, the hacker would need to both use it and know your password to gain entry to your account.

Two-factor authentication is available on both user and admin accounts. But before you enable two-factor authentication on an administrator account, you need to ensure you have a second administrator account configured to guarantee administrator access to the FortiGate unit if you are unable to authenticate on the main admin account for some reason.

Two-factor authentication does not work with explicit proxies.

The methods of two-factor authentication include:

- Certificate
- Email
- SMS
- FortiToken

Certificate

You can increase security by requiring both certificate and password authentication for PKI users. Certificates are installed on the user's computer. Requiring a password also protects against unauthorized use of that computer.

Optionally peer users can enter the code from their FortiToken instead of the certificate.

To create a peer user with two-factor authentication - CLI example

```
config user peer
   edit peer1
      set subject E=peer1@mail.example.com
      set ca CA_Cert_1
      set two-factor enable
      set passwd fdktguefheygfe
   end
```

For more information on certificates, see Certificates overview on page 515.

Email

Two-factor email authentication sends a randomly generated six digit numeric code to the specified email address. Enter that code when prompted at logon. This token code is valid for 60 seconds. If you enter this code after that time,it will not be accepted.

A benefit is that you do not require mobile service to authenticate. However, a potential issue is if your email server does not deliver the email before the 60 second life of the token expires.

The code will be generated and emailed at the time of logon, so you must have email access at that time to be able to receive the code.

To configure an email provider - web-based manager:

1. Go to **System > Config > Advanced > Email Service**.
2. Enter **SMTP Server** and **Default Reply To** address.
3. If applicable, enable **Authentication** and enter the **SMTP User** and **Password** to use.
4. Select a **Security Mode**, options are: **None**, **SMTPS** or **STARTTLS**.
5. Enter the **Port** number, the default is 25.
6. Select **Apply**.

To configure an email provider - CLI:

```
config system email-server
   set server <server_domain-name>
   set reply-to <Recipient_email_address>
end
```

To enable email two-factor authentication - web-based manager:

1. To modify an administrator account, go to **System > Admin > Administrators**. To modify a user account go to **User & Device > User > User Definition**.
2. Edit the user account.
3. Enable and enter the user's **Email Address**.
4. Select **Enable Two-factor Authentication**.
5. Select **Email based two-factor authentication**.
6. Select **OK**.

If **Email based two-factor authentication** option doesn't appear after selecting **Enable Two-factor Authentication**, you need to enable it via the CLI as follows.

To enable email two-factor authentication - CLI:

```
config user local
   edit <user_name>
      set email-to <user_email>
      set two-factor email
   end
```

SMS

SMS two-factor authentication sends the token code in an SMS text message to the mobile device indicated when this user attempts to logon. This token code is valid for 60 seconds. If you enter this code after that time, it will not be accepted. Enter this code when prompted at logon to be authenticated.

SMS two-factor authentication has the benefit that you do not require email service before logging on. A potential issue is if the mobile service provider does not send the SMS text message before the 60 second life of the token expires.

FortiGuard Messaging Service include 4 SMS Messages at no cost. If you need more, you should acquire a license through support.fortinet.com or via customer service.

If you do not use the FortiGuard Messaging Service, you need to configure an SMS service.

To configure an SMS service for your FortiGate unit - web-based manager:

1. Go to **System > Config > Advanced**.
2. In **SMS Service**, select **Create New**.
3. Enter a **Name** for the SMS service and the service **Address** (domain name), then select **OK**.
4. Select **Apply**.

To configure an SMS service - CLI:

```
config system sms-server
   edit <provider_name>
      set mail-server <server_domain-name>
   next
end
```

To configure SMS two-factor authentication - web-based manager:

1. To modify an:
   - administrator account, go to **System > Admin > Administrators, or**
   - user account go to **User & Device > User > User Definition**.
2. Edit the user account.
3. Select SMS and either:
   - Select **FortiGuard Messaging Service**
     or
   - Select **Custom** and then choose the **SMS Provider** to use.
4. Select the **Country/Region**.
5. Enter the phone number of the mobile device that will receive the SMS text messages.
6. Select **Enable Two-factor Authentication**.
7. Select **SMS based two-factor authentication**.
8. Select **OK**.

If **SMS based two-factor authentication** option doesn't appear after selecting **Enable Two-factor Authentication**, you need to enable it via the CLI as follows.

To enable SMS two-factor authentication - CLI:

```
config user local
   edit <user_name>
      set sms-phone <user_phone>
      set sms-server fortiguard
      set two-factor sms
   end
```

If you have problems receiving the token codes via SMS messaging, contact your mobile provider to ensure you are using the correct phone number format to receive text messages and that your current mobile plan allows text messages.

FortiToken

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes every 60 seconds, and when not in use the LCD screen is blanked to extend the battery life.

There is also a mobile phone application, FortiToken Mobile, that performs much the same function.

FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

Any time information about the FortiToken is transmitted, it is encrypted. When the FortiGate unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPsec VPN, SSL VPN, and even Administrators. See Associating FortiTokens with accounts on page 474.

A FortiToken can be associated with only one account on one FortiGate unit.

If a user loses their FortiToken, it can be locked out using the FortiGate so it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiGate to allow access once again. See FortiToken maintenance on page 475.

There are three tasks to complete before FortiTokens can be used to authenticate accounts:

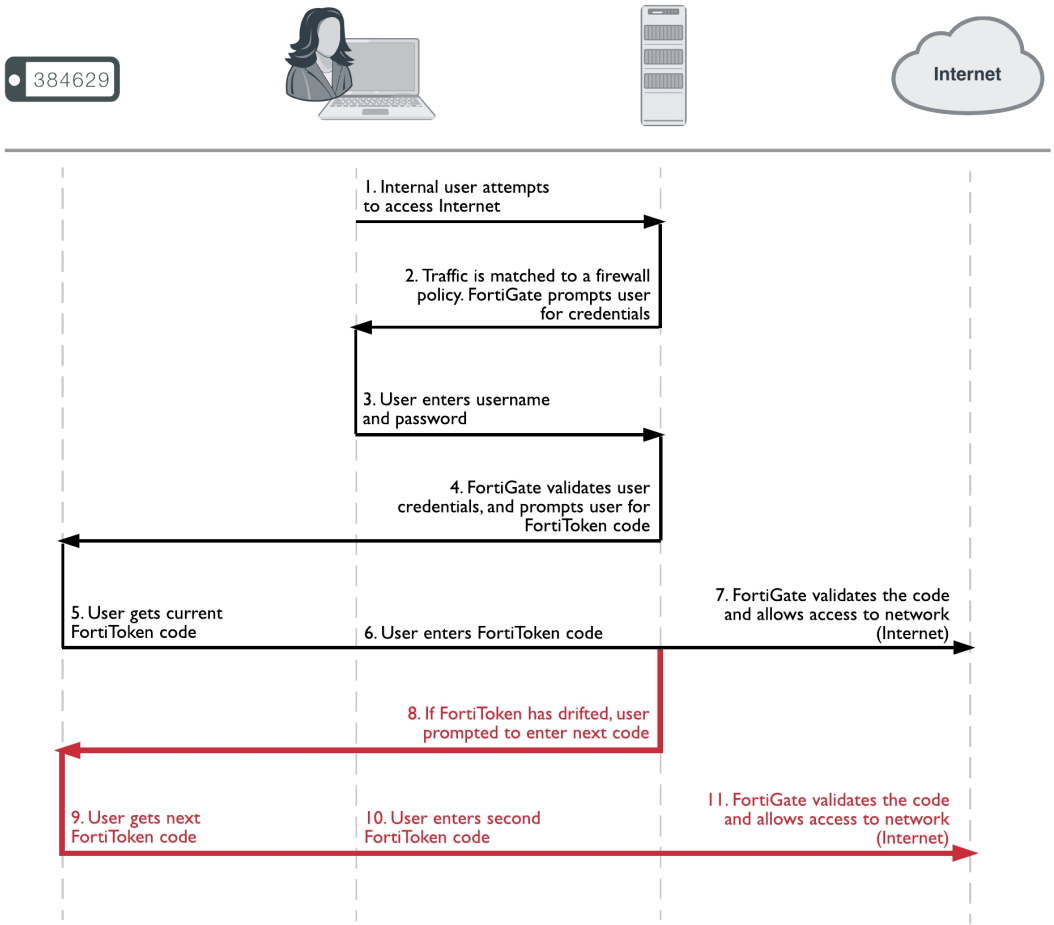
1. Adding FortiTokens to the FortiGate
2. Activating a FortiToken on the FortiGate
3. Associating FortiTokens with accounts

The FortiToken authentication process

The steps during FortiToken two-factor authentication are as follows.

1. User attempts to access a network resource.
2. FortiGate unit matches the traffic to an authentication security policy, and FortiGate unit prompts the user for username and password.
3. User enters their username and password.
4. FortiGate unit verifies their information, and if valid prompts the user for the FortiToken code.
5. User gets the current code from their FortiToken device.
6. User enters current code at the prompt.
7. FortiGate unit verifies the FortiToken code, and if valid allows access to the network resources such as the Internet.
   The following steps are needed only if the time on the FortiToken has drifted and needs to be re-synchronized with the time on the FortiGate unit.
8. If time on FortiToken has drifted, FortiGate unit will prompt user to enter a second code to confirm.
9. User gets the next code from their FortiToken device
10. User enters the second code at the prompt.
11. FortiGate unit uses both codes to update its clock to match the FortiToken and then proceeds as in step "Users and user groups" on page 463.

The FortiToken authentication process is illustrated below:



When configured the FortiGate unit accepts the username and password, authenticates them either locally or remotely, and prompts the user for the FortiToken code. The FortiGate then authenticates the FortiToken code. When FortiToken authentication is enabled, the prompt field for entering the FortiToken code is automatically added to the authentication screens.

Even when an Administrator is logging in through a serial or Telnet connection and their account is linked to a FortiToken, that Administrator will be prompted for the token's code at each login.

If you have attempted to add invalid FortiToken serial numbers, there will be no error message. The serial numbers will simply not be added to the list.

Adding FortiTokens to the FortiGate

Before one or more FortiTokens can be used to authenticate logons, they must be added to the FortiGate. The import feature is used to enter many FortiToken serial numbers at one time. The serial number file must be a text file with one FortiToken serial number per line.

One FortiToken can be added to multiple FortiGate units. This is useful for maintaining two-factor authentication for employees over multiple office locations, such as for employees who travel frequently between offices.

To manually add a FortiToken to the FortiGate - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select **Create New**.
3. In **Type**, select **Hard Token** or **Mobile Token**.
4. Enter one or more FortiToken serial numbers (hard token) or activation codes (mobile token).
5. Select **OK**.

For mobile token, you receive the activation code in the license certificate once you purchase a license. FortiOS include a license for two mobile token at no cost.

To import multiple FortiTokens to the FortiGate - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select **Create New**.
3. In **Type**, select **Hard Token**.
4. Select **Import**.
5. Select **Serial Number File** or **Seed File**, depending on which file you have.
6. Browse to the local file location on your local computer.
7. Select **OK**.
   The file is imported.
8. Select **OK**.

To add two FortiTokens to the FortiGate - CLI:

```
config user fortitoken
   edit <serial_number>
   next
   edit <serial_number2>
   next
end
```

Activating a FortiToken on the FortiGate

Once one or more FortiTokens have been added to the FortiGate unit, they must be activated before being available to be associated with accounts.The process of activation involves the FortiGate querying FortiGuard servers about the validity of each FortiToken. The serial number and information is encrypted before it is sent for added security.

A FortiGate unit requires a connection to FortiGuard servers to activate a FortiToken.

To activate a FortiToken on the FortiGate unit - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select one or more FortiTokens with a status of Available.

3. Right-click the FortiToken entry and select **Activate**.
4. Select **Refresh**.
   The status of selected FortiTokens will change to Activated.

The selected FortiTokens are now available for use with user and admin accounts.

To activate a FortiToken on the FortiGate unit - CLI:

```
config user fortitoken
   edit <token_serial_num>
      set status activate
   next
end
```

Associating FortiTokens with accounts

The final step before using the FortiTokens to authenticate logons is associating a FortiToken with an account. The accounts can be local user or administrator accounts.

To add a FortiToken to a local user account - web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Available.
2. Go to **User & Device > User > User Definition**, and edit the user account.
3. Select **Email Address** and enter user's email address.
4. Select **Enable Two-factor Authentication**.
5. Select the user's FortiToken serial number from the **Token** list.
6. Select **OK**.

For mobile token, click on **Send Activation Code**to be sent to the email address configured previously. The user will use this code to activate his mobile token. An **Email Service** has to be set under **System > Config > Advanced**in order to send the activation code.

To add a FortiToken to a local user account - CLI:

```
config user local
   edit <username>
      set type password
      set passwd "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
      set status enable
   next
   end
```

To add a FortiToken to an administrator account - web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Available.
2. Go to **System > Admin > Administrators**, and edit the admin account.
   This account is assumed to be configured except for two-factor authentication.
3. Select **Email Address** and enter admin's email address.
4. Select **Enable Two-factor Authentication**.
5. Select the user's FortiToken serial number from the **Token** list.
6. Select **OK**.

For mobile token, click on **Send Activation Code**to be sent to the email address configured previously. The admin will use this code to activate his mobile token. An **Email Service** has to be set under **System > Config > Advanced**in order to send the activation code.

To add a FortiToken to an administrator account - CLI:

```
config system admin
   edit <username>
      set password "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
   next
   end
```

The `fortitoken` keyword will not be visible until `fortitoken` is selected for the `two-factor` option.

Before a new FortiToken can be used, it may need to be synchronized due to clock drift.

FortiToken maintenance

Once FortiTokens are entered into the FortiGate unit, there are only two tasks to maintain them — changing the status,

To change the status of a FortiToken between Activated and Locked - CLI:

```
config user fortitoken
   edit <token_serial_num>
      set status lock
   next
end
```

Any user attempting to login using this FortiToken will not be able to authenticate.

To list the drift on all FortiTokens configured on this FortiGate unit - CLI:

```
# diag fortitoken info
```

```
FORTITOKEN DRIFT STATUS
FTK2000BHV1KRZCC 0 token already activated, and seed won't be returned
FTK2001C5YCRRVEE 0 token already activated, and seed won't be returned
FTKMOB4B94972FBA 0 provisioned
FTKMOB4BA4BE9B84 0 new
Total activated token: 0
Total global activated token: 0
Token server status: reachable
```

This command lists the serial number and drift for each FortiToken configured on this FortiGate unit. This command is useful to check if it is necessary to synchronize the FortiGate and any particular FortiTokens.

Monitoring users

To monitor user activity in the web-based manager, go to **User & Device > Monitor > Firewall**. The list of users who are logged on is displayed with some information about them such as their user group, security policy ID, how long they have been logged on, their IP address, traffic volume, and their authentication method as one of FSSO, NTLM, or firewall (FW-auth).

From this screen you can de-authenticate all users who are logged on. The de-authenticate button is at the top left of this screen.

To see information about banned users go to **User & Device > Monitor > Banned User**. Displayed information about users who have been banned includes what application the triggered the ban (Application Protocol), the reason for the ban (Cause or rule), Created, and when the ban expires.

Filtering the list of users

When there are many users logged on, it can be difficult to locate a specific user or multiple users to analyze. Applying filters to the list allows you to organize the user list to meet your needs, or only display some the users that meet your current requirements.

Select settings bottom at the top right of the screen to adjust columns that are displayed for users, including what order they are displayed in. This can be very helpful in locating information you are looking for.

Each column heading has a grey filter icon. Click on the filter icon to configure a filter for the data displayed in that column. Each column has similar options including a field to enter the filtering information, a check box to select the negative of the text in the field, and the options to add more fields, apply the filter, clear all filters, or cancel without saving. To enter multiple terms in the field, separate each of them with a comma. To filter entries that contain a specific prefix, use an * (asterisk).

For example, to create a filter to display only users with an IP address of `10.11.101.x` who authenticated using one of security policies five through eight, and who belong to the user group `Accounting`.

1. Go to **User & Device > Monitor > Firewall**.
2. Select the filter icon beside **IP address**.
3. Enter `10.11.101.` and select **Apply**.
4. Select the filter icon beside **Policy ID.**
5. Enter `5-8` and select **Apply**.
6. Select the filter icon beside **User Group.**
7. Enter `Accounting` and select **Apply**.

User groups

A user group is a list of user identities. An identity can be:

- a local user account (username/password stored on the FortiGate unit
- a remote user account (password stored on a RADIUS, LDAP, or TACACS+ server)
- a PKI user account with digital client authentication certificate stored on the FortiGate unit
- a RADIUS, LDAP, or TACACS+ server, optionally specifying particular user groups on that server
- a user group defined on an FSSO server.

Security policies and some types of VPN configurations allow access to specified user groups only. This restricted access enforces Role Based Access Control (RBAC) to your organization's network and its resources. Users must be in a group and that group must be part of the security policy.

In most cases, the FortiGate unit authenticates users by requesting their username and password. The FortiGate unit checks local user accounts first. If a match is not found, the FortiGate unit checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when a matching username and password are found. If the user belongs to multiple groups on a server, those groups will be matched as well.

FortiOS does not allow username overlaps between RADIUS, LDAP, or TACACS+ servers.

There are four types of FortiGate user groups: Firewall, Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO) user groups.

Firewall user groups

Firewall user groups are used locally as part of authentication. When a security policy allows access only to specified user groups, users must authenticate. If the user authenticates successfully and is a member of one of the permitted groups, the session is allowed to proceed.

This section includes:

- SSL VPN access
- IPsec VPN access
- Configuring a firewall user group
- Multiple group enforcement support
- User group timeouts

SSL VPN access

SSL VPN settings include a list of the firewall user groups that can access the SSL VPN and the SSL VPN portal that each group will use. When the user connects to the FortiGate unit via HTTPS on the SSL VPN port (default 10443), the FortiGate unit requests a username and password.

SSL VPN access also requires a security policy where the destination is the SSL interface. For more information, see the FortiOS Handbook SSL VPN guide.

IPsec VPN access

A firewall user group can provide access for dialup users of an IPsec VPN. In this case, the IPsec VPN phase 1 configuration uses the **Accept peer ID in dialup group** peer option. The user's VPN client is configured with the username as peer ID and the password as pre-shared key. The user can connect successfully to the IPsec VPN only if the username is a member of the allowed user group and the password matches the one stored on the FortiGate unit.

A user group cannot be used as a dialup group if any member of the group is authenticated using an external authentication server.

For more information, see the FortiOS Handbook IPsec VPN guide.

Configuring a firewall user group

A user group can contain:

- local users, whether authenticated by the FortiGate unit or an authentication server
- PKI users
- authentication servers, optionally specifying particular user groups on the server

To create a Firewall user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a name for the user group.
3. In **Type**, select **Firewall**.
4. Add user names to to the **Members** list.
5. Add authentication servers to the **Remote groups** list.
   By default all user accounts on the authentication server are members of this FortiGate user group. To include only specific user groups from the authentication server, deselect **Any** and enter the group name in the appropriate format for the type of server. For example, an LDAP server requires LDAP format, such as: cn=users,dn=office,dn=example,dn=com
   Remote servers must already be configured in **User & Device > Authentication**.
6. Select **OK**.

To create a firewall user group - CLI example:

In this example, the members of `accounting_group` are `User1` and all of the members of `rad_accounting_group` on `myRADIUS` external RADIUS server.

```
config user group
   edit accounting_group
      set group-type firewall
      set member User1 myRADIUS
      config match
         edit 0
            set server-name myRADIUS
            set group-name rad_accounting_group
         end
```

```
end
```

Matching user group names from an external authentication server might not work if the list of group memberships for the user is longer than 8000 bytes. Group names beyond this limit are ignored.

`server_name` is the name of the RADIUS, LDAP, or TACACS+ server, but it must be a member of this group first and must also be a configured remote server on the FortiGate unit.

`group_name` is the name of the group on the RADIUS, LDAP, or TACACS+ server such as “engineering” or “cn=users,dc=test,dc=com”.

Before using group matching with TACACS+, you must first enable authentication. For example if you have a configured TACACS+ server called myTACS, use the following CLI commands.

```
config user tacacs+
   edit myTACS
   set authorization enable
   next
end
```

For more information about user group CLI commands, see the Fortinet CLI Guide.

Multiple group enforcement support

Previously, when a user belonged to multiple user groups, this user could only access the group services that were within one group. With multiple group enforcement, a user can access the services within the groups that the user is part of.

For example, `userA` belongs to `user_group1`, `user_group2`, `user_group3`, and `user_group4`; previously `userA` could only access services within one of those four groups, typically the group that matches the first security policy. This can be annoying if HTTP access is in `user_group1`, FTP access is in `user_group2`, and email access is in `user_group3`. Now `userA` can access services within `user_group1`, `user_group2`, `user_group3`, and `user_group4`.

This feature is available only in the CLI and is enabled by default. It applies to RADIUS, LDAP, and TACACS+ servers. The new command for this feature is `auth-multi-group` found in `config user settings` and checks all groups a user belongs to for authentication.

User group timeouts

User groups can have timeout values per group in addition to FortiGate-wide timeouts. There are essentially three different types of timeouts that are configurable for user authentication on the FortiGate unit — idle timeout, hard timeout, and session timeout. These are in addition to any external timeouts such as those associated with RADIUS servers.

If VDOMs are enabled, the global level user setting `authtimeout` is the default all VDOMs inherit. If VDOMs are not enabled, user settings authtimeout is the default. The default timeout value is used when the `authtimeout` keyword for a user group is set to zero.

Each type of timeout will be demonstrated using the existing user group `example_group`. Timeout units are minutes. A value of zero indicates the global timeout is used.

Membership in multiple groups

When a user belongs to multiple groups in RADIUS groups, the group auth-timeout values are ignored. Instead the global timeout value is used. The default value is 5 minutes, but it can be set from 1 to 1440 minutes (24 hours).

```
config user setting
   set auth-timeout-type idle-timeout
   set auth-timeout 300
end
```

Idle timeout

The default type of timeout is idle timeout. When a user initiates a session, it starts a timer. As long as data is transferred in this session, the timer continually resets. If data flow stops, the timer is allowed to advance until it reaches its limit. At that time the user has been idle for too long, and the user is forced to re-authenticate before traffic is allowed to continue in that session.

To configure user group authentication idle timeout - CLI:

```
config user settings
   set auth-timeout-type idle-timeout
end
config user group
   edit example_group
      set authtimeout 5 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

Hard timeout

Where the idle timeout is reset with traffic, the hard timeout is absolute. From the time the first session a user establishes starts, the hard timeout counter starts. When the timeout is reached, all the sessions for that user must be re-authenticated. This timeout is not affected by any event.

To configure user group authentication hard timeout - CLI:

```
config user settings
   set auth-timeout-type hard-timeout
end
config user group
   edit example_group
      set authtimeout 1440 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

Session timeout

The session timeout works much like the hard timeout in that its an absolute timer that can not be affected by events. However, when the timeout is reached existing sessions may continue but new sessions are not allowed until re-authentication takes place.

To configure a user group authentication new session hard timeout - CLI:

```
config user setting
   set auth-timeout-type new-session
end

config user group
   edit example_group
      set authtimeout 30 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

SSO user groups

SSO user groups are part of FSSO authentication and contain only Windows or Novell network users. No other user types are permitted as members. Information about the Windows or Novell user groups and the logon activities of their members is provided by the Fortinet Single Sign On (FSSO) which is installed on the network domain controllers.

You can specify FSSO user groups in security policies in the same way as you specify firewall user groups. FSSO user groups cannot have SSL VPN or dialup IPsec VPN access.

For information about configuring FSSO user groups, see Creating Fortinet Single Sign-On (FSSO) user groups on page 582. For complete information about installing and configuring FSSO, see Agent-based FSSO on page 545.

Configuring Peer user groups

Peer user groups can only be configured using the CLI. Peers are digital certificate holders defined using the `config user peer` command. The peer groups you define here are used in dialup IPsec VPN configurations that accept RSA certificate authentication from members of a peer certificate group.

To create a peer group - CLI example:

```
config user peergrp
   edit vpn_peergrp1
      set member pki_user1 pki_user2 pki_user3
   end
```

Viewing, editing and deleting user groups

To view the list of FortiGate user groups, go to **User & Device > User > User Groups**.

Editing a user group

When editing a user group in the CLI you must set the type of group this will be — either a firewall group, a Fortinet Single Sign-On Service group (FSSO), a Radius based Single Sign-On Service group (RSSO), or a guest group. Once the type of group is set, and members are added you cannot change the group type without removing the members.

In the web-based manager, if you change the type of the group any members will be removed automatically.

To edit a user group - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select the user group that you want to edit.
3. Select the **Edit** button.
4. Modify the user group as needed.
5. Select **OK**.

To edit a user group - CLI example:

This example adds user3 to Group1. Note that you must re-specify the full list of users:

```
config user group
   edit Group1
   set group-type firewall
      set member user2 user4 user3
   end
```

Deleting a user group

Before you delete a user group, you must ensure there are no objects referring to, it such as security policies. If there are, you must remove those references before you are able to delete the user group.

To remove a user group - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select the user group that you want to remove.
3. Select the **Delete** button.
4. Select **OK**.

To remove a user group - CLI example:

```
config user group
   delete Group2
end
```

Managing Guest Access

Visitors to your premises might need user accounts on your network for the duration of their stay. If you are hosting a large event such as a conference, you might need to create many such temporary accounts. The FortiOS Guest Management feature is designed for this purpose.

A guest user account User ID can be the user's email address, a randomly generated string, or an ID that the administrator assigns. Similarly, the password can be administrator-assigned or randomly generated.

You can create many guest accounts at once using randomly-generated User IDs and passwords. This reduces administrator workload for large events.

User's view of guest access

1. The user receives an email, SMS message, or printout from a FortiOS administrator listing a User ID and password.
2. The user logs onto the network with the provided credentials.
3. After the expiry time, the credentials are no longer valid.

Administrator's view of guest access

1. Create one or more guest user groups.
   All members of the group have the same characteristics: type of User ID, type of password, information fields used, type and time of expiry.
2. Create guest accounts using Guest Management.
3. Use captive portal authentication and select the appropriate guest group.

Configuring guest user access

To set up guest user access, you need to create at least one guest user group and add guest user accounts. Optionally, you can create a guest management administrator whose only function is the creation of guest accounts in specific guest user groups. Otherwise, any administrator can do guest management.

Creating guest management administrators

To create a guest management administrator

1. Go to **System > Admin > Administrators** and create a regular administrator account.
   For detailed information see the System Administration chapter.
2. Select **Restrict to Provision Guest Accounts**.
3. In **Guest Groups**, add the guest groups that this administrator manages.

Creating guest user groups

The guest group configuration determines the fields that are provided when you create a guest user account.

To create a guest user group:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information:

Name	Enter a name for the group.
Type	Guest
Enable Batch Account Creation	Create multiple accounts automatically. When this is enabled: • **User ID** and **Password** are set to **Auto-Generate**. • The user accounts have only **User ID, Password**, and **Expiration** fields. Only the **Expiration** field is editable. If the expiry time is a duration, such as "8 hours", this is the time after first login. • You can print the account information. Users do not receive email or SMS notification. See To create multiple guest user accounts automatically on page 485.
User ID	Select one of: • Email — User's email address • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random user ID
Password	Select one of: • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random password • Disable — no password
Expire Type	Choose one of: • Immediately — expiry time is counted from creation of account • After first login — expiry time is counted from user's first login
Default Expire Time	Set the expire time. The administrator can change this for individual users.
Enable Name	If enabled, user must provide a name.
Enable Sponsor	If enabled, user form has Sponsor field. Select **Required** if required.
Enable Company	If enabled, user form has Company field. Select **Required**if required.
Enable Email	If enabled, user is notified by email.
Enable SMS	If enabled, user is notified by SMS. Select whether FortiGuard Messaging Service or a another SMS provider is used. You can add SMS providers in **System > Config > Messaging Servers**.

Creating guest user accounts

Guest user accounts are not the same as local user accounts created in **User & Device > User > User Definition**. Guest accounts are not permanent; they expire after a defined time period. You create guest accounts in **User & Device > User > Guest Management**.

To create a guest user account

1. Go to **User & Device > User > Guest Management.**
2. In **Guest Groups**, select the guest group to manage.

3. Select **Create New** and fill in the fields in the **New User** form.
   Fields marked Optional can be left blank. The guest group configuration determines the fields that are available.
4. Select **OK**.

To create multiple guest user accounts automatically

1. Go to **User & Device > User > Guest Management.**
2. In **Guest Groups**, select the guest group to manage.
   The guest group must have the **Enable Batch Guest Account Creation** option enabled.
3. Select **Create New > Multiple Users**.
   Use the down-pointing caret to the right of **Create New**.
4. Enter **Number of Accounts**.
5. Optionally, change the **Expiration**.
6. Select **OK**.

Guest Management Account List

Go to **User & Device > User > Guest Management** to create, view, edit or delete guest user accounts.

Create New	Creates a new guest user account.
Edit	Edit the selected guest user account.
Delete	Delete the selected guest user account.
Purge	Remove all expired accounts from the list.
Send	Send the user account information to a printer or to the guest. Depending on the group settings and user information, the information can be sent to the user by email or SMS.
Refresh	Update the list.
Guest Groups	Select the guest group to list. New accounts are added to this group.
User ID	The user ID. Depending on the guest group settings, this can be the user's email address, an ID that the administrator specified, or a randomly-generated ID.
Expires	Indicates a duration such as "3 hours". A duration on its own is relative to the present time. Or, the duration is listed as "after first login."

Guest access in a retail environment

Some retail businesses such as coffee shops provide free Wi-Fi Internet access for their customers. For this type of application, the FortiOS guest management feature is not required; the Wi-Fi access point is open and customers do not need logon credentials. However, the business might want to contact its customers later with promotional offers to encourage further patronage. Using an Email Collection portal, it is possible to collect customer email addresses for this purpose. The security policy grants network access only to users who provide a valid email address.

The first time a customer's device attempts to use the Wi-Fi connection, FortiOS requests an email address, which it validates. The customer's subsequent connections go directly to the Internet without interruption.

Creating an email harvesting portal

The customer's first contact with your network will be with a captive portal which presents a web page requesting an email address. When FortiOS has validated the email address, the customer's device MAC address is added to the Collected Emails device group.

To create the email collection portal:

1. Go to **WiFi & Switch Controller > WiFi Network > SSID** and edit your SSID.
2. Set **Security Mode** to **Captive Portal**.
3. Set **Portal Type** to **Email Collection**.
4. Optionally, in **Customize Portal Messages** select **Email Collection.**

You can change the portal content and appearance. See Customizing captive portal pages on page 508.

To create the email collection portal - CLI:

In this example the `freewifi` Wi-Fi interface is modified to present an email collection captive portal.

```
config wireless-controller vap
   edit freewifi
      set security captive-portal
      set portal-type email-collect
end
```

Creating the security policy

You need configure a security policy that allows traffic to flow from the Wi-Fi SSID to the Internet interface but only for members of the Collected Emails device group. This policy must be listed first. Unknown devices are not members of the Collected Emails device group, so they do not match the policy.

To create the security policy:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	freewifi
Source Address	all
Source Device Type	Collected Emails
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL

Action	ACCEPT
NAT	On

3. Select **OK**.

To create the authentication rule - CLI:

```
config firewall policy
   edit 3
      set srcintf "freewifi"
      set dstintf "wan1"
      set srcaddr "all"
      set action accept
      set devices collected-emails
      set nat enable
      set schedule "always"
      set service "ALL"
   end
```

Checking for harvested emails

In the web-based manager, go to **User & device > Device > Device Definitions**. In the CLI you can use the `diagnose user device list` command. For example,

```
FGT-100D # diagnose user device list
hosts
   vd 0 d8:d1:cb:ab:61:0f gen 35 req 30 redir 1 last 43634s 7-11_2-int
      ip 10.0.2.101 ip6 fe80::dad1:cbff:feab:610f
      type 2 'iPhone' src http c 1 gen 29
      os 'iPhone' version 'iOS 6.0.1' src http id 358 c 1
      email 'yo@yourdomain.com'
   vd 0 74:e1:b6:dd:69:f9 gen 36 req 20 redir 0 last 39369s 7-11_2-int
      ip 10.0.2.100 ip6 fe80::76e1:b6ff:fedd:69f9
      type 1 'iPad' src http c 1 gen 5
      os 'iPad' version 'iOS 6.0' src http id 293 c 1
      host 'Joes's-iPad' src dhcp
      email 'you@fortinet.com'
```

Fall-through authentication policies

User authentication policies have an implicit fall-through feature that intentionally causes policy matching to fall through to a policy lower on the list that can also match the traffic. In other words the first user policy that is matched in the policy list, based on standard policy criteria, isn't the only policy that can be matched.

Fall-through is intended to match users in different user groups with different policies. For example, consider an organization with two user groups where one group requires a web filtering profile, while the other requires virus scanning. In this example, you would edit two basic Internet access policies: policy 1 assigning **User Group A** with a **Web Filtering** profile, and policy 2 assigning **User Group B** with an **AntiVirus** profile. Both policies are also assigned to the same internal subnet, named **subnet1**.

In this configuration, all users from **subnet1** will see an authentication prompt. If the user is found in **User Group A**, the traffic is accepted by policy 1 and is filtered by the **Web Filtering** profile. If the user is found in **User Group B**, the traffic is accepted by policy 2 and is virus scanned.

The fall-through feature is required for users to be matched with policy 2. Without the fall-through feature, traffic would never be matched with policy 2.

Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure security policies and certain types of VPNs to require user authentication.

This section describes:

- Authentication timeout
- Password policy
- Authentication protocols
- Authentication in Captive Portals
- Authentication in security policies
- VPN authentication

Authentication timeout

An important feature of the security provided by authentication is that it is temporary—a user must re-authenticate after logging out. Also if a user is logged on and authenticated for an extended period of time, it is a good policy to have them re-authenticate at set periods. This ensures a user's session is cannot be spoofed and used maliciously for extended periods of time — re-authentication will cut any spoof attempts short. Shorter timeout values are more secure.

Security authentication timeout

You set the security user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 1440 minutes (24 hours).

To set the security authentication timeout - web-based manager:

1. Go to **User & Device > Authentication > Settings**.
2. Enter the **Authentication Timeout** value in minutes.
   The default authentication timeout is 5 minutes.
3. Select **Apply**.

SSL VPN authentication timeout

You set the SSL VPN user authentication timeout (**Idle Timeout**) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 259 200 seconds. The default timeout is 300 seconds.

To set the SSL VPN authentication timeout - web-based manager:

1. Go to **VPN > SSL > Settings**.
2. Under **Idle Logout**, make sure that **Logout users when inactive for specified period** is enabled and enter the **Inactive For** value (seconds).
3. Select **Apply**.

Password policy

Password authentication is effective only if the password is sufficiently strong and is changed periodically. By default, the FortiGate unit requires only that passwords be at least eight characters in length. You can set a password policy to enforce higher standards for both length and complexity of passwords. Password policies can apply to administrator passwords or IPsec VPN preshared keys.

To set a password policy in the web-based manager, go to **System > Admin > Settings**. In the CLI, use the `config system password-policy` command.

The default minimum password length on the FortiGate unit is eight characters, but up to 128 characters is permitted.

Users usually create passwords composed of alphabetic characters and perhaps some numbers. Password policy can require the inclusion of uppercase letters, lowercase letters, numerals or punctuation characters.

Configuring password minimum requirement policy

Best practices dictate that passwords include:

- one or more uppercase characters
- one or more lower case characters
- one or more of the numerals
- one or more special characters.

The minimum number of each of these types of characters can be set in both the web-based manager and the CLI.

The following procedures show how to force administrator passwords to contain at least two uppercase, four lower care, two digits, and one special character. Leave the minimum length at the default of eight characters.

To change administrator password minimum requirements - web-based manager:

1. Go to **System > Admin > Settings**.
2. Select **Enable Password Policy**.
3. Select **Must Contain at Least**.
4. Enter the following information:

Upper Case Letters	2
Lower Case Letters	4
Numbers	2
Special Characters	1

5. Under **Apply Password Policy to**, select **Administrator Password**.
6. Select **Apply**.

To change administrator password minimum requirements - CLI:

```
config system password-policy
   set status enable
```

```
    set apply-to admin-password
    set min-upper-case-letter 2
    set min-lower-case-letter 4
    set min-number 2
    set min-non-alphanumeric 1
    set change-4-characters enable
end
```

The `change-4-characters` option forces new passwords to change a minimum of four characters in the old password. Changing fewer characters results in the new password being rejected. This option is only available in the CLI.

Password best practices

In addition to length and complexity, there are security factors that cannot be enforced in a policy. Guidelines issued to users will encourage proper password habits.

Best practices dictate that password expiration also be enabled. This forces passwords to be changed on a regular basis. You can set the interval in days. The more sensitive the information this account has access to, the shorter the password expiration interval should be. For example 180 days for guest accounts, 90 days for users, and 60 days for administrators.

Avoid:

- real words found in any language dictionary
- numeric sequences, such as “12345”
- sequences of adjacent keyboard characters, such as “qwerty”
- adding numbers on the end of a word, such as “hello39”
- adding characters to the end of the old password, such as “hello39” to “hello3900”
- repeated characters
- personal information, such as your name, birthday, or telephone number.

Maximum logon attempts and blackout period

When you logon and fail to enter the correct password you could be a valid user, or a hacker attempting to gain access. For this reason, best practices dictate to limit the number of failed attempts to logon before a blackout period where you cannot logon.

To set a maximum of five failed authentication attempts before the blackout, using the following CLI command:

```
config user setting
   set auth-invalid-max 5
end
```

To set the length of the blackout period to five minutes, or 300 seconds, once the maximum number of failed logon attempts has been reached, use the following CLI command:

```
config user setting
   set auth-blackout-time 300
end
```

Authentication protocols

When user authentication is enabled on a security policy, the authentication challenge is normally issued for any of the four protocols, HTTP, HTTPS, FTP, and Telnet, which are dependent on the connection protocol. By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first, so that they can subsequently connect with other protocols.

For example, if you have selected HTTP, FTP, or Telnet, a username and password-based authentication occurs. The FortiGate unit then prompts network users to input their security username and password. If you have selected HTTPS, certificate-based authentication (HTTPS, or HTTP redirected to HTTPS only) occurs.

FTP and Telnet authentication replacement messages cannot be customized. For HTTP and HTTPS replacement messages see Authentication replacement messages on page 493.

For certificate-based authentication, you must install customized certificates on the FortiGate unit and on the browsers of network users. If you do not install certificates on the network user's web browser, the network users may see an SSL certificate warning message and have to manually accept the default FortiGate certificate. The network user's web browser may deem the default certificate as invalid.

When you use certificate authentication, if you do not specify any certificate when you create the security policy, the global settings are used. If you specify a certificate, the per-policy setting will overwrite the global setting. For more information about the use of certification authentication see Certificate-based authentication on page 514.

To set the authentication protocols

1. Go to **User & Device > Authentication > Settings**.
2. In **Protocol Support**, select the required authentication protocols.
3. If using HTTPS protocol support, in **Certificate**, select a Local certificate from the drop-down list.
4. Select **Apply**.

Authentication in Captive Portals

Network interfaces, including WiFi interfaces, can perform authentication at the interface level using a captive portal — an HTML form that requests the user's name and password. A captive portal is useful where all users connecting to the network interface must authenticate. Optionally, on a WiFi interface, the captive portal can be combined with a terms of service disclaimer to which the user must agree before gaining access. For more information, see Captive portals on page 506.

Once successfully authenticated, the user's session passes to the firewall.

Authentication in security policies

Security policies control traffic between FortiGate interfaces, both physical interfaces and VLAN subinterfaces. The firewall tries to match the session's user or group identity, device type, destination, etcetera to a security policy. When a match is found, the user connects to the requested destination. If no security policy matches, the user is denied access.

A user who has not already been authenticated by a captive portal, FSSO, or RSSO can match only policies where no user or user group is specified. If no such policy exists, the firewall requests authentication. If the user can authenticate and the session can be matched to a policy, the user connects to the requested destination, otherwise, the user is denied access.

This section includes:

- Enabling authentication protocols
- Authentication replacement messages
- Access to the Internet
- Configuring authentication security policies
- Identity-based policy
- NTLM authentication
- Certificate authentication
- Restricting number of concurrent user logons

Enabling authentication protocols

Users can authenticate using FTP, HTTP, HTTPS, and Telnet. However, these protocols must be enabled first.

Another authentication option is to redirect any attempts to authenticate using HTTP to a more secure channel that uses HTTPS. This forces users to a more secure connection before entering their user credentials.

To enable support for authentication protocols - web-based manager:

1. Go to **User & Device > Authentication > Settings**.
2. Select one or more of HTTP, HTTPS, FTP, Telnet, or Redirect HTTP Challenge to a Secure Channel (HTTPS). Only selected protocols will be available for use in authentication.
3. Select the **Certificate** to use, for example `Fortinet_Factory`.
4. Select **Apply**.

To enable support for authentication protocols - CLI:

```
config user setting
   set auth-type ftp http https telnet
   set auth-cert Fortinet_Factory
end
```

Authentication replacement messages

A replacement message is the body of a webpage containing a message about a blocked website message, a file too large message, a disclaimer, or even a login page for authenticating. The user is presented with this message instead of the blocked content.

Authentication replacement messages are the prompts a user sees during the security authentication process such as login page, disclaimer page, and login success or failure pages. These are different from most replacement messages because they are interactive requiring a user to enter information, instead of simply informing the user of some event as other replacement messages do.

Replacement messages have a system-wide default configuration, a per-VDOM configuration, and disclaimers can be customized for multiple security policies within a VDOM.

These replacement messages are used for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the security authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

More information about replacement messages can be found in the `config system replacemsg` section of the FortiOS CLI Reference.

List of authentication replacement messages

Replacement message name (CLI name)	Description
Login challenge page (auth-challenge-page)	This HTML page is displayed if security users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, “Please enter new PIN”). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified. The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN. This page uses the %%QUESTION%% tag.
Disclaimer page (auth-disclaimer-page-1) (auth-disclaimer-page-2) (auth-disclaimer-page-3)	This page prompts user to accept the displayed disclaimer when leaving the captive portal to access Internet resources. It is displayed when the captive portal type is **Authentication and Disclaimer** or **Disclaimer Only**. In the CLI, the auth-disclaimer-page-2 and auth-disclaimer-page-3 pages seamlessly extend the size of the disclaimer page from 8 192 characters to 16 384 and 24 576 characters respectively. In the web-based manager this is handled automatically. See Disclaimer on page 498.
Email token page (auth-email-token-page)	The page prompting a user to enter their email token. See Email on page 1.
FortiToken page (auth-fortitoken-page)	The page prompting a user to enter their FortiToken code. See FortiToken on page 470.

Keepalive page (auth-keepalive-page)	The HTML page displayed with security authentication keepalive is enabled using the following CLI command:
	
	`config system globalset auth-keepalive enable`
	`end`
	
	Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. In the web-based manager, go to **User & Device > Authentication > Settings** to set the **Authentication Timeout**.
	
	This page includes %%TIMEOUT%%.

Replacement message name (CLI name)	Description
Login failed page (auth-login-failed-page)	The Disclaimer page replacement message does not re-direct the user to a redirect URL or the security policy does not include a redirect URL. When a user selects the button on the disclaimer page to decline access through the FortiGate unit, the Declined disclaimer page is displayed.
Login page (auth-login-page)	The authentication HTML page displayed when users who are required to authenticate connect through the FortiGate unit using HTTP or HTTPS. Prompts the user for their username and password to login. This page includes %%USERNAMEID%% and %%PASSWORDID%% tags.
Declined disclaimer page (auth-reject-page)	The page displayed if a user declines the disclaimer page. See Disclaimer on page 498.
SMS Token page (auth-sms-token-page)	The page prompting a user to enter their SMS token. See SMS on page 469.
Success message (auth-success-msg)	The page displayed when a user successfully authenticates. Prompts user to attempt their connection again (as the first was interrupted for authentication).

Access to the Internet

A policy for accessing the Internet is similar to a policy for accessing a specific network, but the destination address is set to **all**. The destination interface is the one that connects to the Internet Service Provider (ISP). For general purpose Internet access, the Service is set to ALL.

Access to HTTP, HTTPS, FTP and Telnet sites may require access to a domain name service. DNS requests do not trigger authentication. You must configure a policy to permit unauthenticated access to the appropriate DNS server, and this policy must **precede** the policy for Internet access. Failure to do this will result in the lack of a DNS connection and a corresponding lack of access to the Internet.

Configuring authentication security policies

To include authentication in a security policy, the policy must specify user groups. A security policy can authenticate by certificate, FSSO, and NTLM. The two exceptions to this are RADIUS SSO and FSSO Agents. See SSO using RADIUS accounting records on page 589, and Introduction to FSSO agents on page 546.

Before creating a security policy, you need to configure one or more users or user groups. For more information, see Users and user groups on page 463.

Creating the security policy is the same as a regular security policy except you must select the action specific to your authentication method:

Authentication methods allowed for each policy Action

Action	Authentication method	Where authentication is used
ACCEPT	FSSO Agent or a security policy that specifies an FSSO user group	Agent-based FSSO on page 545.
	NTLM	See NTLM authentication on page 499.
	Certificates	See Configuring certificate-based authentication on page 526.
	RADIUS SSO	See SSO using RADIUS accounting records on page 589.
DENY	none	none

Disclaimer

A WiFi or SSL captive portal can include a disclaimer message presented after the user authenticates. The user must agree to the terms of the disclaimer to access network resources.

Customizing authentication replacement messages

Customizing disclaimers or other authentication replacement messages involves changing the text of the disclaimer message, and possibly the overall appearance of the message.

Changing the disclaimer in **System > Config > Replacement messages** is not the same as selecting to customize a disclaimer used in a captive portal. The **System > Config** location is the default message that all disclaimers inherit. The captive portal location is a customized disclaimer that inherits the default format for the disclaimer message, but then can be customized for this portal.

To customize the disclaimer for a captive portal - web-based manager:

1. Go to **System > Network > Interface**. Either select an existing interface or create a new one.
2. Under **Security Mode**, select **Captive Portal**, and enable **Customize Portal Messages**.
3. Select the **Edit** icon. You can select and edit any of the pages. Change your text or layout as needed.

Enabling security logging

There are two types of logging that relate to authentication — event logging, and security logging.

When enabled, event logging records system events such as configuration changes, and authentication. To configure event logging, go to **Log&Report > Log Config > Log Settings** and enable **Event Logging**. Select the events you want to log, such as **User activity event**.

When enabled, security logging will log security profile and security policy traffic.

You must enable logging within a security policy, as well as the options that are applied to a security policy, such as security profiles features. Event logs are enabled within the Event Log page.

For more information on logging, see the FortiOS Log and Reporting guide.

For more information on specific types of log messages, see the FortiOS Log Message Reference.

You need to set the logging severity level to **Notification** when configuring a logging location to record traffic log messages.

To enable logging within an existing security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4**.
2. Expand to reveal the policy list of a policy.
3. Select the security policy you want to enable logging on and then select **Edit**.
4. To log all general firewall traffic, select the check box beside **Log Allowed Traffic**, and choose to enable **Security Events** or **All Sessions**.
5. Select **OK**.

Identity-based policy

An identity-based policy (IBP) performs user authentication in addition to the normal security policy duties. If the user does not authenticate, access to network resources is refused. This enforces Role Based Access Control (RBAC) to your organization's network and resources.

Identity-based policies also support Single Sign-On operation. The user groups selected in the policy are of the Fortinet Single Sign-On (FSSO) type.

User authentication can occur through any of the following supported protocols, including: HTTP, HTTPS, FTP, and Telnet. The authentication style depends on which of these protocols is included in the selected security services group and which of those enabled protocols the network user applies to trigger the authentication challenge.

For username and password-based authentication (HTTP, FTP, and Telnet) the FortiGate unit prompts network users to enter their username, password, and token code if two-factor authentication is selected for that user account. For certificate-based authentication, including HTTPS or HTTP redirected to HTTPS only, see Certificate authentication on page 500.

With identity-based policies, the FortiGate unit allows traffic that matches the source and destination addresses, device types, and so on. This means specific security policies must be placed **before** more general ones to be effective.

When the identity-based policy has been configured, the option to customize authentication messages is available. This allows you to change the text, style, layout, and graphics of the replacement messages associated with this firewall policy. When enabled, customizing these messages follows the same method as changing the disclaimer. See Disclaimer on page 498.

Types of authentication also available in identity-based policies are

- NTLM authentication
- Certificate authentication

NTLM authentication

NT LAN Manager (NTLM) protocol can be used as a fallback for authentication when the Active Directory (AD) domain controller is unreachable. NTLM uses the web browser to send and receive authentication information. See "NTLM" and "FSSO NTLM authentication support".

To enable NTLM

1. Edit the policy in the CLI to enable NTLM. For example, if the policy ID is 4:
2. Go to **Policy & Objects > Policy > IPv4** and note the **ID** number of your FSSO policy.
3. The policy must have an FSSO user group as **Source User(s)**. There must be at least one FSSO Collector agent configured on the FortiGate unit.

```
config firewall policy
   edit 4
      set ntlm enable
   end
```

NTLM guest access

Guest profile access may be granted to users who fail NTLM authentication, such as visitors who have no user credentials on the network. To allow guest user access, edit the FSSO security policy in the CLI, like this:

```
config firewall policy
   edit 4
      set ntlm enable
      set ntlm-guest enable
   end
```

NTLM enabled browsers - CLI

User agent strings for NTLM enabled browsers allow the inspection of initial HTTP-User-Agent values, so that non-supported browsers are able to go straight to guest access without needlessly prompting the user for credentials that will fail. `ntlm-guest` must be enabled to use this option.

```
config firewall policy
   edit 4
      set ntlm enable
      set ntlm-guest enable
      set ntlm-enabled-browsers <user_agent_string>
   next
   end
```

`<user_agent_string>` is the name of the browser that is NTLM enabled. Examples of these values include “MSIE”, “Mozilla” (which includes FireFox), and “Opera”.

Value strings can be up to 63 characters in length, and may not contain cross site scripting (XSS) vulnerability characters such as brackets. The FortiGate unit prevents use of these characters to prevent exploit of cross site scripting (XSS) vulnerabilities.

Certificate authentication

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users. See Configuring certificate-based authentication on page 526.

Certificates are also inherent to the HTTPS protocol, where the browser validates the server’s identity using certificates. A site certificate must be installed on the FortiGate unit and the corresponding Certificate Authority (CA) certificate installed in the web browser.

To force the use of HTTPS, go to **User & Device > Authentication > Settings** and select **Redirect HTTP Challenge to a Secure Channel (HTTPS)**.

Restricting number of concurrent user logons

Some users on your network may often have multiple account sessions open at one time either to the same network resource or accessing to the admin interface on the FortiGate unit.

While there are valid reasons for having multiple concurrent sessions open, hackers also do this to speed up their malicious work. Often a hacker is making multiple attempts to gain access to the internal network or the admin interface of the FortiGate unit, usually from different IP addresses to appear to the FortiGate unit as legitimate users. For this reason, the more concurrent sessions a hacker has open at once, the faster they will achieve their goal.

To help prevent this, you can disallow concurrent administrative access using the same administrator user name, but from a different IP address. This allows valid users to continue their legitimate work while limiting hackers' activity.

To disable concurrent administrator sessions - CLI:

```
config system global
   set admin-concurrent disable
end
```

VPN authentication

All VPN configurations require users to authenticate. Authentication based on user groups applies to:

- SSL VPNs
- PPTP and L2TP VPNs
- an IPsec VPN that authenticates users using dialup groups
- a dialup IPsec VPN that uses XAUTH authentication (Phase 1)

You must create user accounts and user groups before performing the procedures in this section. If you create a user group for dialup IPsec clients or peers that have unique peer IDs, their user accounts must be stored locally on the FortiGate unit. You cannot authenticate these types of users using a RADIUS or LDAP server.

Configuring authentication of SSL VPN users

The general procedure for authenticating SSL VPN users is:

1. Configure user accounts.
2. Create one or more user groups for SSL VPN users.
3. Enable SSL VPN.
4. Optionally, set inactivity and authentication timeouts.
5. Configure a security policy with the user groups you created for SSL VPN users.
   See FortiOS Handbook SSL VPN guide.

Configuring authentication timeout

By default, the SSL VPN authentication expires after 8 hours (28 800 seconds). You can change it only in the CLI, and the time entered must be in seconds. The maximum time is 72 hours (259 200 seconds). For example, to change this timeout to one hour, you would enter:

```
config vpn ssl settings
   set auth-timeout 3600
end
```

If you set the authentication timeout (`auth-timeout`) to 0 when you configure the timeout settings, the remote client does not have to re-authenticate unless they log out of the system. To fully take advantage of this setting, the value for `idle-timeout` has to be set to 0 also, so that the client does not time out if the maximum idle time is reached. If the `idle-timeout` is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the `auth-timeout` setting.

Configuring authentication of remote IPsec VPN users

An IPsec VPN on a FortiGate unit can authenticate remote users through a dialup group. The user account name is the peer ID and the password is the pre-shared key.

Authentication through user groups is supported for groups containing only local users. To authenticate users using a RADIUS or LDAP server, you must configure XAUTH settings. See Configuring XAuth authentication.

To configure user group authentication for dialup IPsec - web-based manager:

1. Configure the dialup users who are permitted to use this VPN. Create a user group with Type:Firewall and add them to it.
   For more information, see Users and user groups on page 463
2. Go to **VPN > IPsec > Wizard**, select **Dialup**, choose a name for the VPN, and enter the following information.

Incoming Interface	Select the incoming interface name.
Authentication Method	List of authentication methods available for users. Select **Preshared Key** and enter the preshared key.
User Group	Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.

3. Select **Next** and continue configure other VPN parameters as needed.
4. Select **OK**.

To configure user group authentication for dialup IPsec - CLI example:

The `peertype` and `usrgrp` options configure user group-based authentication.

```
config vpn ipsec phase1
   edit office_vpn
      set interface port1
      set type dynamic
      set psksecret yORRAzltNGhzgtV32jend
      set proposal 3des-sha1 aes128-sha1
      set peertype dialup
      set usrgrp Group1
   end
```

Configuring XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication information in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit asks the user for a username

and password. It then forwards the user's credentials (the password is encrypted) to an external RADIUS or LDAP server for verification.

XAuth can be used in addition to or in place of IPsec phase 1 peer options to provide access security through an LDAP or RADIUS authentication server. You must configure a dialup user group whose members are all externally authenticated.

To configure authentication for a dialup IPsec VPN - web-based manager:

1. Configure the users who are permitted to use this VPN. Create a user group and add the users to the group. For more information, see "Users and user groups" on page 463.
2. Go to **VPN > IPsec > Wizard**, select **Dialup**, choose a name for the VPN, and enter the following information.

Incoming Interface	Select the incoming interface name.
Authentication Method	List of authentication methods available for users. Select **Preshared Key** and enter the preshared key.
User Group	Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.

3. Select **Next** and continue configure other VPN parameters as needed.
4. Select **OK**.
5. Go to **VPN > IPsec > Tunnels**, edit the Tunnel just created, select **Convert To Custom Tunnel**, and edit **XAUTH** as following:

Type	Select **PAP**, **CHAP**, or **AUTO**. Use CHAP whenever possible. Use PAP with all implementations of LDAP and with other authentication servers that do not support CHAP, including some implementations of Microsoft RADIUS. Use AUTO with the Fortinet Remote VPN Client and where the authentication server supports CHAP but the XAuth client does not.
User Group	Select the user group that is to have access to the VPN. The list of user groups does not include any group that has members whose password is stored on the FortiGate unit.

6. Select **OK**.

For more information about XAUTH configuration, see the IPsec VPN chapter of the FortiOS Handbook.

To configure authentication for a dialup IPsec VPN - CLI example:

The `xauthtype` and `authusrgrp` fields configure XAuth authentication.

```
config vpn ipsec phase1
   edit office_vpn
      set interface port1
      set type dynamic
      set psksecret yORRAzltNGhzgtV32jend
      set proposal 3des-sha1 aes128-sha1
      set peertype dialup
      set xauthtype pap
      set usrgrp Group1
   end
```

Some parameters specific to setting up the VPN itself are not shown here. For detailed information about configuring IPsec VPNs, see the FortiOS Handbook IPsec VPN guide.

Configuring authentication of PPTP VPN users and user groups

Configuration of a PPTP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

To configure authentication for a PPTP VPN

1. Configure the users who are permitted to use this VPN. Create a security user group and add them to it. For more information, see Users and user groups on page 463.
2. Configure the PPTP VPN in the CLI as in this example.

```
config vpn pptp
   set status enable
   set sip 192.168.0.100
   set eip 192.168.0.110
   set usrgrp PPTP_Group
end
```

The `sip` and `eip` fields define a range of virtual IP addresses assigned to PPTP clients.

Configure a security policy. The source interface is the one through which the clients will connect. The source address is the PPTP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.

Configuring authentication of L2TP VPN users/user groups

Configuration of a L2TP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

To configure authentication for a L2TP VPN

1. Configure the users who are permitted to use this VPN. Create a user group and add them to it. For more information, see Users and user groups on page 463.
2. Configure the L2TP VPN in the CLI as in this example.

```
config vpn l2tp
   set status enable
   set sip 192.168.0.100
```

```
        set eip 192.168.0.110
        set usrgrp L2TP_Group
    end
```

The `sip` and `eip` fields define a range of virtual IP addresses assigned to L2TP clients.

3. Configure a security policy. The source interface is the one through which the clients will connect. The source address is the L2TP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.

Captive portals

A captive portal is a convenient way to authenticate web users on wired or WiFi networks.

This section describes:

- Introduction to Captive Portals
- Configuring a captive portal
- Customizing captive portal pages

Introduction to Captive Portals

You can authenticate your users on a web page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. This is called a captive portal.

After successful authentication, the user accesses the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access to only the members of specified user group.

The captive portal can be hosted on the FortiGate unit or on an external authentication server. You can configure captive portal authentication on any network interface, including WiFi and VLAN interfaces.

When a captive portal is configured on a WiFi interface, the access point initially appears open. The wireless client can connect to the access point with no security credentials, but sees only the captive portal authentication page.

WiFi captive portal types:

- **Authentication** — until the user enters valid credentials, no communication beyond the AP is permitted.
- **Disclaimer + Authentication** — immediately after successful authentication, the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding.
- **Disclaimer Only** — the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding. The authentication page is not presented.
- **Email Collection** — the portal presents a page requesting the user's email address, for the purpose of contacting the person in future. This is often used by businesses who provide free WiFi access to their customers. The authentication page is not presented.

Configuring a captive portal

Captive portals are configured on network interfaces. On a physical (wired) network interface, you edit the interface configuration in **System > Network > Interfaces** and set **Security Mode** to **Captive Portal**. A WiFi interface does not exist until the WiFi SSID is created. You can configure a WiFi captive portal at the time that you create the SSID. Afterwards, the captive portal settings will also be available by editing the WiFi network interface in **System > Network > Interfaces**.

To configure a wired Captive Portal - web-based manager:

1. Go to **System > Network > Interfaces** and edit the interface to which the users connect.
2. In **Security Mode** select **Captive Portal**.

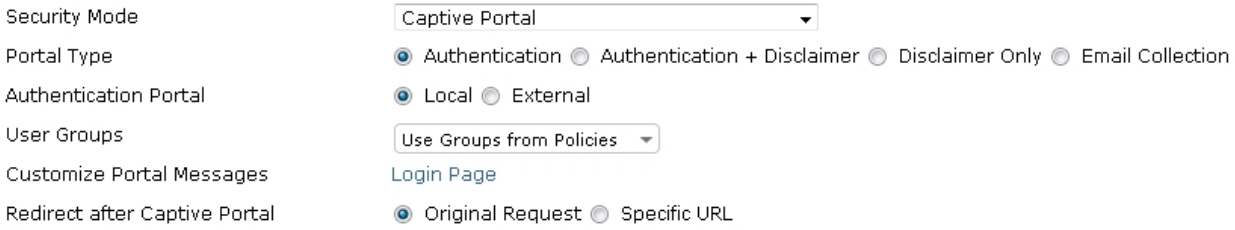
3. Enter

Authentication Portal	Local - portal hosted on the FortiGate unit. Remote - enter FQDN or IP address of external portal.
User Groups	Select permitted user groups or select **Use Groups from Policies**, which permits the groups specified in the security policy. **Use Groups from Policies** is not available in WiFi captive portals.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Enable, then select Edit. See Customizing captive portal pages on page 508.

4. Select **OK**.

To configure a WiFi Captive Portal - web-based manager:

1. Go to **WiFi Controller > WiFi Network > SSID** and create your SSID.
   If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **System > Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.



3. Enter

Portal Type	The portal can provide authentication and/or disclaimer, or perform user email address collection. See Introduction to Captive Portals on page 506.
Authentication Portal	Local - portal hosted on the FortiGate unit. Remote - enter FQDN or IP address of external portal.

User Groups	Select permitted user groups.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Click the link of the portal page that you want to modify. See "Captive portals" on page 508.

4. Select **OK**.

Exemption from the captive portal

A captive portal requires all users on the interface to authenticate. But some devices are not able to authenticate. You can create an exemption list of these devices. For example, a printer might need to access the Internet for firmware upgrades. Using the CLI, you can create an exemption list to exempt all printers from authentication.

```
config user security-exempt-list
   edit r_exempt
      config rule
         edit 1
            set devices printer
         end
      end
```

Customizing captive portal pages

These pages are defined in replacement messages. Defaults are provided. In the web-based manager, you can modify the default messages in the SSID configuration by selecting **Customize Portal Messages**. Each SSID can have its own unique portal content.

The captive portal contains the following default web pages:

- **Login page**—requests user credentials

Typical modifications for this page would be to change the logo and modify some of the text.

You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

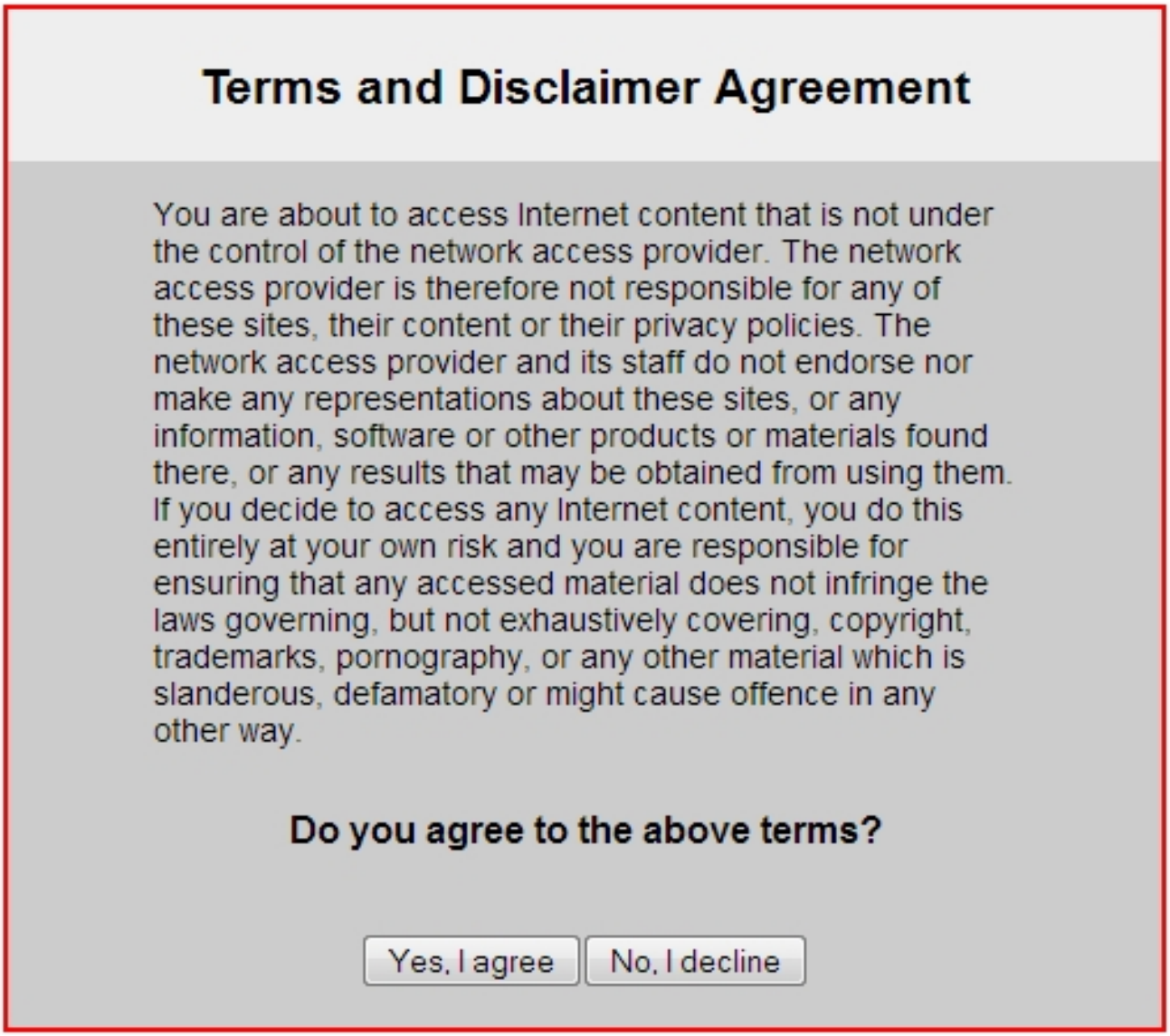
There is an exception to this rule. The line “Please enter your credentials to continue” is provided by the %%QUESTION%% tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Login failed page**—reports that the entered credentials were incorrect and enables the user to try again.

The Login failed page is similar to the Login page. It even contains the same login form. You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

There is an exception to this rule. The line “Firewall authentication failed. Please try again.” is provided by the %%FAILED_MESSAGE%% tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Disclaimer page**—is a statement of the legal responsibilities of the user and the host organization to which the user must agree before proceeding.(WiFi or SSL VPN only)



- **Declined disclaimer page**—is displayed if the user does not agree to the statement on the Disclaimer page. Access is denied until the user agrees to the disclaimer.

Changing images in portal messages

You can replace the default Fortinet logo with your organization's logo. First, import the logo file into the FortiGate unit and then modify the Login page code to reference your file.

To import a logo file:

1. Go to **System > Config > Replacement Messages** and select **Manage Images**.
2. Select **Create New**.
3. Enter a **Name** for the logo and select the appropriate **Content Type**.
   The file must not exceed 24 Kilo bytes.
4. Select **Browse**, find your logo file and then select **Open**.
5. Select **OK**.

To specify the new logo in the replacement message:

1. Go to **System > Network > Interfaces** and edit the interface.
   The **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
   - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
   - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. In the HTML message text, find the %%IMAGE tag.
   By default it specifies the Fortinet logo: `%%IMAGE:logo_fw_auth%%`
4. Change the image name to the one you provided for your logo.
   The tag should now read, for example, `%%IMAGE:mylogo%%`
5. Select **Save**.
6. Select **OK**.

Modifying text in portal messages

Generally, you can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters. You should not remove any tags because they may carry information that the FortiGate unit needs. See the preceding section for any exceptions to this rule for particular pages.

To modify portal page text

1. Go to **System > Network > Interfaces** and edit the interface.
   The SSID **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
   - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
   - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. Edit the HTML message text, then select **Save**.
4. Select **OK**.

Configuring disclaimer page for ethernet interface captive portals

While you can customize a disclaimer page for captive portals that connect via WiFi, the same can be done for wired connections. However, this can only be configured on the CLI Console, and only without configuring user groups.

When configuring a captive portal through the CLI, you may `set security-groups` to a specific user group. The result of this configuration will show an authentication form to users who wish to log in to the captive portal—**not** a disclaimer page. If you do not set any `security-groups` in your configuration, an "Allow all" status will be in effect, and the disclaimer page will be displayed for users.

The example CLI configuration below shows setting up a captive portal interface without setting security-groups, resulting in a disclaimer page for users:

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 172.16.101.1 255.255.255.0
      set allowaccess ping https ssh snmp http
      set type physical
      set explicit-web-proxy enable
      set alias "LAN"
      set security-mode captive-portal
      set snmp-index 1
   next
end
```

Certificate-based authentication

This section provides an overview of how the FortiGate unit verifies the identities of administrators, SSL VPN users, or IPsec VPN peers using X.509 security certificates.

The following topics are included in this section:

- What is a security certificate?
- Certificates overview
- Managing X.509 certificates
- Configuring certificate-based authentication
- Example — Generate a CSR on the FortiGate unit
- Example — Generate and Import CA certificate with private key pair on OpenSSL
- Example — Generate an SSL certificate in OpenSSL

What is a security certificate?

A security certificate is a small text file that is part of a third-party generated public key infrastructure (PKI) to help guarantee the identity of both the user logging on and the web site they where they are logging in.

A certificate includes identifying information such as the company and location information for the web site, as well as the third-party company name, the expiry date of the certificate, and the public key.

FortiGate units use X.509 certificates to authenticate single sign-on (SSO) for users. The X.509 standard has been in use since before 2000, but has gained popularity with the Internet's increased popularity. X.509 v3 is defined in RFC 5280 and specifies standard formats for public key certificates, certificate revocation lists, and a certification path validation algorithm. The unused earlier X.509 version 1 was defined in RFC 1422.

The main difference between X.509 and PGP certificates is that where in PGP anyone can sign a certificate, for X.509 only a trusted authority can sign certificates. This limits the source of certificates to well known and trustworthy sources. Where PGP is well suited for one-to-one communications, the X.509 infrastructure is intended to be used in many different situations including one-to-many communications. Some common filename extensions for X.509 certificates are listed below.

Common certificate filename extensions

Filetype	Format name	Description
.pem	Privacy Enhanced Mail (PEM)	Base64 encoded DER certificate, that uses: "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
.cer **.crt** **.der**	Security CERtificate	Usually binary DER form, but Base64-encoded certificates are common too.
.p7b **.p7c**		Structure without data, just certificates or CRLs. PKCS#7 is a standard for signing or encrypting (officially called "enveloping") data.
.p12	PKCS#12	May contain certificate(s) (public) and private keys (password protected).
.pfx	personal information exchange (PFX)	Older format. Came before PKCS#12. Usually today data is in PKCS#12 format.

Certificates overview

Certificates play a major role in authentication of clients connecting to network services via HTTPS, both for administrators and SSL VPN users. Certificate authentication is optional for IPsec VPN peers.

- Certificates and protocols
- IPsec VPNs and certificates
- Certificate types on the FortiGate unit

Certificates and protocols

There are a number of protocols that are commonly used with certificates including SSL and HTTPS, and other certificate-related protocols.

SSL and HTTPS

The secure HTTP (HTTPS) protocol uses SSL. Certificates are an integral part of SSL. When a web browser connects to the FortiGate unit via HTTPS, a certificate is used to verify the FortiGate unit's identity to the client. Optionally, the FortiGate unit can require the client to authenticate itself in return.

By default, the FortiGate unit uses a self-signed security certificate to authenticate itself to HTTPS clients. When the certificate is offered, the client browser displays two security messages.

- The first message prompts users to accept and optionally install the FortiGate unit's self-signed security certificate. If the user does not accept the certificate, the FortiGate unit refuses the connection. When the user accepts the certificate, the FortiGate login page is displayed, and the credentials entered by the user are encrypted before they are sent to the FortiGate unit. If the user chooses to install the certificate, the prompt is not displayed again.

- Just before the FortiGate login page is displayed, a second message informs users that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit redirects the connection (away from the distinguished name recorded in the self-signed certificate) and can be ignored.

Optionally, you can install an X.509 server certificate issued by a certificate authority (CA) on the FortiGate unit. You can then configure the FortiGate unit to identify itself using the server certificate instead of the self-signed certificate.

For more information, see the FortiOS Handbook SSL VPN guide.

After successful certificate authentication, communication between the client browser and the FortiGate unit is encrypted using SSL over the HTTPS link.

Certificate-related protocols

There are multiple protocols that are required for handling certificates. These include the Online Certificate Status Protocol (OCSP), Secure Certificate Enrollment Protocol (SCEP), and Server-based Certificate Validation Protocol (SCVP).

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) allows the verification of X.509 certificate expiration dates. This is important to prevent hackers from changing the expiry date on an old certificate to a future date.

Normally certificate revocation lists (CRLs) are used, but OCSP is an alternate method available. However a CRL is a public list, and some companies may want to avoid the public exposure of their certificate structure even if it is only invalid certificates.

The OSCP check on the certificate's revocation status is typically carried out over HTTP with a request-response format. The authority responding can reply with a status of good, revoked, or unknown for the certificate in question.

Secure Certificate Enrollment Protocol

Secure Certificate Enrollment Protocol (SCEP) is an automated method of signing up for certificates. Typically this involves generating a request you send directly to the SCEP service, instead of generating a file request that may or may not be signed locally.

Server-based Certificate Validation Protocol

Server-based Certificate Validation Protocol (SCVP) is used to trace a certificate back to a valid root level certificate. This ensures that each step along the path is valid and trustworthy.

IPsec VPNs and certificates

Certificate authentication is a more secure alternative to preshared key (shared secret) authentication for IPsec VPN peers. Unlike administrators or SSL VPN users, IPsec peers use HTTP to connect to the VPN gateway configured on the FortiGate unit. The VPN gateway configuration can require certificate authentication before it permits an IPsec tunnel to be established. See Authenticating IPsec VPN users with security certificates on page 527 .

Certificate types on the FortiGate unit

There are different types of certificates available that vary depending on their intended use. FortiOS supports local, remote, CA, and CRL certificates.

Local certificates

Local certificates are issued for a specific server, or web site. Generally they are very specific, and often for an internal enterprise network. For example a personal web site for John Smith at www.example.com (such as http://www.example.com/home/jsmith) would have its own local certificate.

These can optionally be just the certificate file, or also include a private key file and PEM passphrase for added security.

For information about generating a certificate request, see Generating a certificate signing request on page 518. For information about installing a local certificate, see Obtaining and installing a signed server certificate from an external CA on page 521

Remote certificates

Remote certificates are public certificates without a private key. For dynamic certificate revocation, you need to use an Online Certificate Status Protocol (OCSP) server. The OCSP is configured in the CLI only. Installed Remote (OCSP) certificates are displayed in the Remote Certificates list. You can select **Import** to install a certificate from the management PC.

CA root certificates

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of www.example.com instead of just the smaller single web page.

Certificate revocation list

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

Certificate signing

The trust in a certificate comes from the authority that signs it. For example if VeriSign signs your CA root certificate, it is trusted by everyone. While these certificates are universally accepted, it is cumbersome and expensive to have all certificates on a corporate network signed with this level of trust.

With self-signed certificates nobody, except the other end of your communication, knows who you are and therefore they do not trust you as an authority. However this level is useful for encryption between two points — neither point may care about who signed the certificate, just that it allows both points to communicate. This is very useful for internal networks and communications.

A general rule is that CA signed certificates are accepted and sometimes required, but it is easier to self-sign certificates when you are able.

For more on the methods of certificate signing see Generating a certificate signing request on page 518.

Managing X.509 certificates

Managing security certificates is required due to the number of steps involved in both having a certificate request signed, and then distributing the correct files for use.

You use the FortiGate unit or CA software such as OpenSSL to generate a certificate request. That request is a text file that you send to the CA for verification, or alternately you use CA software to self-validate. Once validated, the certificate file is generated and must be imported to the FortiGate unit before it can be used. These steps are explained in more detail later in this section.

This section provides procedures for generating certificate requests, installing signed server certificates, and importing CA root certificates and CRLs to the FortiGate unit.

For information about how to install root certificates, CRLs, and personal or group certificates on a remote client browser, refer to your browser's documentation.

This section includes:

- Generating a certificate signing request
- Generating certificates with CA software
- Obtaining and installing a signed server certificate from an external CA
- Installing a CA root certificate and CRL to authenticate remote clients
- Troubleshooting certificates
- Online updates to certificates and CRLs
- Backing up and restoring local certificates

Generating a certificate signing request

Whether you create certificates locally with a software application or obtain them from an external certificate service, you will need to generate a certificate signing request (CSR).

When you generate a CSR, a private and public key pair is created for the FortiGate unit. The generated request includes the public key of the FortiGate unit and information such as the FortiGate unit's public static IP address, domain name, or email address. The FortiGate unit's private key remains confidential on the FortiGate unit.

After you submit the request to a CA, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate, and you install the certificate on the FortiGate unit.

The Certificate Request Standard is a public key cryptography standard (PKCS) published by RSA, specifically PKCS10 which defines the format for CSRs. This is defined in RFC 2986.

To generate a certificate request in FortiOS - web-based manager:

1. Go to **System > Certificates > Local Certificates**.
2. Select **Generate**.
3. In the **Certificate Name** field, enter a unique meaningful name for the certificate request. Typically, this would be the hostname or serial number of the FortiGate unit or the domain of the FortiGate unit such as example.com.

Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

4. Enter values in the **Subject Information** area to identify the FortiGate unit:
   - If the FortiGate unit has a static IP address, select **Host IP**and enter the public IP address of the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or fully qualified domain name (FQDN) if available) instead.
   - If the FortiGate unit has a dynamic IP address and subscribes to a dynamic DNS service, use a FQDN if available to identify the FortiGate unit. If you select **Domain Name**, enter the FQDN of the FortiGate unit. Do not include the protocol specification (http://) or any port number or path names.

If a domain name is not available and the FortiGate unit subscribes to a dynamic DNS service, an “unable to verify certificate” type message may be displayed in the user’s browser whenever the public IP address of the FortiGate unit changes.

   - If you select **E-Mail**, enter the email address of the owner of the FortiGate unit.
5. Enter values in the **Optional Information** area to further identify the FortiGate unit.

Organization Unit	Name of your department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icon.
Organization	Legal name of your company or organization.
Locality (City)	Name of the city or town where the FortiGate unit is installed.
State/Province	Name of the state or province where the FortiGate unit is installed.
Country	Select the country where the FortiGate unit is installed.
e-mail	Contact email address.
Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: IP:1.1.1.1 email:test@fortinet.com email:my@other.address URI:http://my.url.here/

6. From the **Key Type** list, select **RSA** or **Elliptic Curve**.
7. From the **Key Size** list, select **1024 Bit**, **1536 Bit**, **2048 Bit** or **secp256r1**, **secp384r1**, **secp521r1** respectively. Larger keys are slower to generate but more secure.
8. In **Enrollment Method**, you have two methods to choose from. Select **File Based** to generate the certificate request, or **Online SCEP** to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.
9. Select **OK**.
10. The request is generated and displayed in the **Local Certificates** list with a status of `PENDING`.
11. Select the **Download** button to download the request to the management computer.
12. In the **File Download** dialog box, select **Save** and save the Certificate Signing Request on the local file system of the management computer.
13. Name the file and save it on the local file system of the management computer.

The certificate request is ready for the certificate authority to be signed.

Generating certificates with CA software

CA software allows you to generate unmanaged certificates and CA certificates for managing other certificates locally without using an external CA service. Examples of CA software include ssl-ca from OpenSSL (available for Linux, Windows, and Mac) or gensslcert from SuSE, MS Windows Server 2000 and 2003 come with a CA as part of their certificate services, and in MS Windows 2008 CA software can be installed as part of the Active Directory installation. See Example — Generate and Import CA certificate with private key pair on OpenSSL on page 529.

The general steps for generating certificates with CA software are

1. Install the CA software as a stand-alone root CA.
2. Provide identifying information for your self-administered CA.

While following these steps, the methods vary slightly when generating server certificates, CA certificates, and PKI certificates.

Server certificate

1. Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2. Copy the CSR base-64 encoded text (PKCS10 or PKCS7) into the CA software and generate the certificate. PKCS10 is the format used to send the certificate request to the signing authority. PKCS7 is the format the signing authority can use for the newly signed certificate.
3. Export the certificate as a X.509 DER encoded binary file with .CER extension
4. Upload the certificate file to the FortiGate unit Local Certificates page (type is Certificate).

CA certificate

1. Retrieve the CA Certificate from the CA software as a DER encoded file.
2. Import the CA certificate file to the FortiGate unit at **System > Certificates > Import > CA Certificates**.

PKI certificate

1. Generate a Certificate Signing Request (CSR) on the FortiGate unit.

2. Copy the CSR base-64 encoded text (PKCS#10 or PKCS#7) into the CA software and generate the certificate. PKCS10 is the format used to send the certificate request to the signing authority. PKCS7 is the format the signing authority can use for the newly signed certificate.
3. Export the certificate as a X.509 DER encoded binary file with .CER extension.
4. Install the certificate in the user's web browser or IPsec VPN client as needed.

Obtaining and installing a signed server certificate from an external CA

To obtain a signed server certificate for a FortiGate unit, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request.

To submit the certificate signing request (file-based enrollment):

1. Using the web browser on the management computer, browse to the CA web site.
2. Follow the CA instructions for a base-64 encoded PKCS#10 certificate request and upload your certificate request.
3. Follow the CA instructions to download their root certificate and CRL.
   When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit.

To install or import the signed server certificate - web-based manager

1. On the FortiGate unit, go to **System > Certificates > Import > Local Certificates**.
2. From **Type**, select **Local Certificate**.
3. Select **Browse**, browse to the location on the management computer where the certificate was saved, select the certificate, and then select **Open**.
4. Select **OK**, and then select **Return**.

Installing a CA root certificate and CRL to authenticate remote clients

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and CRL from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit according to the procedures given below.

To install a CA root certificate

1. After you download the root certificate of the CA, save the certificate on the management computer. Or, you can use online SCEP to retrieve the certificate.
2. On the FortiGate unit, go to **System > Certificates > Import > CA Certificates**.
3. Do one of the following:
   - To import using SCEP, select **SCEP**. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the filename.
   - To import from a file, select **Local PC**, then select **Browse** and find the location on the management computer where the certificate has been saved. Select the certificate, and then select **Open**.
5. Select **OK**, and then select **Return**.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

To import a certificate revocation list

A Certificate Revocation List (CRL) is a list of the CA certificate subscribers paired with certificate status information. The list contains the revoked certificates and the reason(s) for revocation. It also records the certificate issue dates and the CAs that issued them.

When configured to support SSL VPNs, the FortiGate unit uses the CRL to ensure that the certificates belonging to the CA and remote peers or clients are valid. The CRL has an “effective date” and a “next update” date. The interval is typically 7 days (for Microsoft CA). FortiOS will update the CRL automatically. Also, there is a CLI command to specify an “update-interval” in seconds. Recommendation should be 24 hours (86400 seconds) but depends on company security policy.

1. After you download the CRL from the CA web site, save the CRL on the management computer.
2. Go to **System > Certificates > Import > CRL**.
3. Do one of the following:
   - To import using an HTTP server, select **HTTP** and enter the URL of the HTTP server.
   - To import using an LDAP server see this KB article.
   - To import using an SCEP server, select **SCEP** and select the Local Certificate from the list. Enter the URL of the SCEP server from which the CRL can be retrieved.
   - To import from a file, select **Local PC**, then select **Browse** and find the location on the management computer where the CRL has been saved. Select the CRL and then select **Open**.
5. Select **OK**, and then select **Return**.

Troubleshooting certificates

There are times when there are problems with certificates — a certificate is seen as expired when its not, or it can’t be found. Often the problem is with a third party web site, and not FortiOS. However, some problems can be traced back to FortiOS such as DNS or routing issues.

Certificate is reported as expired when it is not

Certificates often are issued for a set period of time such as a day or a month, depending on their intended use. This ensures everyone is using up-to-date certificates. It is also more difficult for hackers to steal and use old certificates.

Reasons a certificate may be reported as expired include:

- It really has expired based on the “best before” date in the certificate
- The FortiGate unit clock is not properly set. If the FortiGate clock is fast, it will see a certificate as expired before the expiry date is really here.
- The requesting server clock is not properly set. A valid example is if your certificate is 2 hours from expiring, a server more than two time zones away would see the certificate as expired. Otherwise, if the server’s clock is set wrongly it will also have the same effect.
- The certificate was revoked by the issuer before the expiry date. This may happen if the issuer believes a certificate was either stolen or misused. Its possible it is due to reasons on the issuer’s side, such as a system change or such. In either case it is best to contact the certificate issuer to determine what is happening and why.

A secure connection cannot be completed (Certificate cannot be found)

Everyone who uses a browser has encountered a message such as *This connection is untrusted*. Normally when you try to connect securely to a web site, that web site will present its valid certificate to prove their identity is valid. When the web site's certificate cannot be verified as valid, the message appears stating *This connection is untrusted* or something similar. If you usually connect to this web site without problems, this error could mean that someone is trying to impersonate or hijack the web site, and best practices dictates you not continue.

Reasons a web site's certificate cannot be validated include:

- The web site uses an unrecognized self-signed certificate. These are not secure because anyone can sign them. If you accept self-signed certificates you do so at your own risk. Best practices dictate that you must confirm the ID of the web site using some other method before you accept the certificate.
- The certificate is valid for a different domain. A certificate is valid for a specific location, domain, or sub-section of a domain such as one certificate for `support.example.com` that is not valid for `marketing.example.com`. If you encounter this problem, contact the webmaster for the web site to inform them of the problem.
- There is a DNS or routing problem. If the web site's certificate cannot be verified, it will not be accepted. Generally to be verified, your system checks with the third party certificate signing authority to verify the certificate is valid. If you cannot reach that third party due to some DNS or routing error, the certificate will not be verified.
- Firewall is blocking required ports. Ensure that any firewalls between the requesting computer and the web site allow the secure traffic through the firewall. Otherwise a hole must be opened to allow it through. This includes ports such as 443 (HTTPS) and 22 (SSH).

Online updates to certificates and CRLs

If you obtained your local or CA certificate using SCEP, you can configure online renewal of the certificate before it expires. Similarly, you can receive online updates to CRLs.

Local certificates

In the `config vpn certificate local` command, you can specify automatic certificate renewal. The relevant fields are:

`scep-url <URL_str>`	The URL of the SCEP server. This can be HTTP or HTTPS. The following options appear after you add the `<URL_str>`.
`scep-password <password_str>`	The password for the SCEP server.
`auto-regenerate-days <days_int>`	How many days before expiry the FortiGate unit requests an updated local certificate. The default is `0`, no auto-update.
`auto-regenerate-days-warning <days_int>`	How many days before local certificate expiry the FortiGate generates a warning message. The default is `0`, no warning.

In this example, an updated certificate is requested three days before it expires.

```
config vpn certificate local
   edit mycert
      set scep-url http://scep.example.com/scep
      set scep-server-password my_pass_123
      set auto-regenerate-days 3
```

```
      set auto-regenerate-days-warning 2
   end
```

CA certificates

In the `config vpn certificate ca` command, you can specify automatic certificate renewal. The relevant fields are:

Variable	Description
`scep-url <URL_str>`	The URL of the SCEP server. This can be HTTP or HTTPS.
`auto-update-days <days_int>`	How many days before expiry the FortiGate unit requests an updated CA certificate. The default is `0`, no auto-update.
`auto-update-days-warning <days_int>`	How many days before CA certificate expiry the FortiGate generates a warning message. The default is `0`, no warning.

In this example, an updated certificate is requested three days before it expires.

```
config vpn certificate ca
   edit mycert
      set scep-url http://scep.example.com/scep
      set auto-update-days 3
      set auto-update-days-warning 2
   end
```

Certificate Revocation Lists

If you obtained your CRL using SCEP, you can configure online updates to the CRL using the `config vpn certificate crl` command. The relevant fields are:

Variable	Description
`http-url <http_url>`	URL of the server used for automatic CRL certificate updates. This can be HTTP or HTTPS.
`scep-cert <scep_certificate>`	Local certificate used for SCEP communication for CRL auto-update.
`scep-url <scep_url>`	URL of the SCEP CA server used for automatic CRL certificate updates. This can be HTTP or HTTPS.
`update-interval <seconds>`	How frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter `0` to update the CRL only when it expires. Not available for http URLs.
`update-vdom <update_vdom>`	VDOM used to communicate with remote SCEP server for CRL auto-update.

In this example, an updated CRL is requested only when it expires.

```
config vpn certificate crl
   edit cert_crl
```

```
    set http-url http://scep.example.com/scep
    set scep-cert my-scep-cert
    set scep-url http://scep.ca.example.com/scep
    set update-interval 0
    set update-vdom root
end
```

Backing up and restoring local certificates

The FortiGate unit provides a way to export and import a server certificate and the FortiGate unit's personal key through the CLI. If required (to restore the FortiGate unit configuration), you can import the exported file through the **System > Certificates** page of the web-based manager.

As an alternative, you can back up and restore the entire FortiGate configuration through the **System Information** widget on the Dashboard of the web-based manager. Look for **[Backup]** and **[Restore]** in the **System Configuration** row. The backup file is created in a FortiGate-proprietary format.

To export a server certificate and private key - CLI:

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate unit before you enter the command.

1. Connect to the FortiGate unit through the CLI.
2. Type the following command:

   ```
   execute vpn certificate local export tftp <cert_name> <exp_filename> <tftp_ip>
       <password>
   ```

   where:

   - `<cert_name>` is the name of the server certificate; typing `?` displays a list of installed server certificates.
   - `<exp_filename>` is a name for the output file.
   - `<tftp_ip>` is the IP address assigned to the TFTP server host interface.
3. Move the output file from the TFTP server location to the management computer for future reference.

To import a server certificate and private key - web-based manager:

1. Go to **System > Certificates** and select **Import**.
2. In **Type**, select **PKCS12 Certificate**.
3. Select **Browse**. Browse to the location on the management computer where the exported file has been saved, select the file, and then select **Open**.
4. In the **Password** field, type the password needed to upload the exported file.
5. Select **OK**, and then select **Return**.

To import separate server certificate and private key files - web-based manager

Use the following procedure to import a server certificate and the associated private key file when the server certificate request and private key were not generated by the FortiGate unit. The two files to import must be available on the management computer.

1. Go to **System > Certificates** and select **Import**.
2. In **Type**, select **Certificate**.

3. Select the **Browse** button beside the **Certificate file** field. Browse to the location on the management computer where the certificate file has been saved, select the file, and then select **Open**.
4. Select the **Browse** button beside the **Key file** field. Browse to the location on the management computer where the key file has been saved, select the file, and then select **Open**.
5. If required, in the **Password** field, type the associated password, and then select **OK**.
6. Select **Return**.

Configuring certificate-based authentication

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users.

In Microsoft Windows 7, you can use the certificate manager to keep track of all the different certificates on your local computer. To access certificate manager, in Windows 7 press the Windows key, enter “certmgr.msc” at the search prompt, and select the displayed match. Remember that in addition to these system certificates, many applications require you to register certificates with them directly.

To see FortiClient certificates, open the FortiClient Console, and select VPN. The VPN menu has options for My Certificates (local or client) and CA Certificates (root or intermediary certificate authorities). Use Import on those screens to import certificate files from other sources.

Authenticating administrators with security certificates

You can install a certificate on the management computer to support strong authentication for administrators. When a personal certificate is installed on the management computer, the FortiGate unit processes the certificate after the administrator supplies a username and password.

To enable strong administrative authentication:

- Obtain a signed personal certificate for the administrator from a CA and load the signed personal certificate into the web browser on the management computer according to the browser documentation.
- Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see Installing a CA root certificate and CRL to authenticate remote clients on page 521).
- Create a PKI user account for the administrator.
- Add the PKI user account to a firewall user group dedicated to PKI-authenticated administrators.
- In the administrator account configuration, select **PKI** as the account **Type** and select the **User Group** to which the administrator belongs.

Authenticating SSL VPN users with security certificates

While the default self-signed certificates can be used for HTTPS connections, it is preferable to use the X.509 server certificate to avoid the redirection as it can be misinterpreted as possible session hijacking. However, the server certificate method is more complex than self-signed security certificates. Also the warning message is typically displayed for the initial connection, and future connections will not generate these messages.

X.509 certificates can be used to authenticate IPsec VPN peers or clients, or SSL VPN clients. When configured to authenticate a VPN peer or client, the FortiGate unit prompts the VPN peer or client to authenticate itself using the X.509 certificate. The certificate supplied by the VPN peer or client must be verifiable using the root CA certificate installed on the FortiGate unit in order for a VPN tunnel to be established.

To enable certificate authentication for an SSL VPN user group:

1. Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
2. Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.
3. Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see Installing a CA root certificate and CRL to authenticate remote clients on page 521).
4. Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
5. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the SSL VPN users who are authenticated by certificate.
6. Go to **Policy & Objects > Policy > IPv4**.
7. Edit the SSL-VPN security policy.
8. Select the user group created earlier in the **Source User(s)** field.
9. Select **OK**.

Authenticating IPsec VPN users with security certificates

To require VPN peers to authenticate by means of a certificate, the FortiGate unit must offer a certificate to authenticate itself to the peer.

To enable the FortiGate unit to authenticate itself with a certificate:

1. Install a signed server certificate on the FortiGate unit.
   See To install or import the signed server certificate - web-based manager on page 521.
2. Install the corresponding CA root certificate on the remote peer or client. If the remote peer is a FortiGate unit, see To install a CA root certificate on page 521.
3. Install the certificate revocation list (CRL) from the issuing CA on the remote peer or client. If the remote peer is a FortiGate unit, see To import a certificate revocation list on page 522.
4. In the VPN phase 1 configuration, set **Authentication Method** to **Signature** and from the **Certificate Name** list select the certificate that you installed in Step 1.

To authenticate a VPN peer using a certificate, you must install a signed server certificate on the peer. Then, on the FortiGate unit, the configuration depends on whether there is only one VPN peer or if this is a dialup VPN that can be multiple peers.

To configure certificate authentication of a single peer

1. Install the CA root certificate and CRL.
2. Create a PKI user to represent the peer. Specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
3. In the VPN phase 1 **Peer Options**, select **peer certificate** for **Accept Types** field and select the PKI user that you created in the **Peer certificate** field.

To configure certificate authentication of multiple peers (dialup VPN)

1. Install the corresponding CA root certificate and CRL.
2. Create a PKI user for each remote VPN peer. For each user, specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
3. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the PKI users who will use the IPsec VPN.

In the VPN phase 1 **Peer Options**, select **peer certificate group** for **Accept Types** field and select the PKI user group that you created in the **Peer certificate group** field.

Example — Generate a CSR on the FortiGate unit

This example follows all the steps required to create and install a local certificate on the FortiGate unit, without using CA software.

The FortiGate unit is called myFortiGate60, and is located at 10.11.101.101 (a private IP address) and http://myfortigate.example.com. Mr. John Smith (john.smith@myfortigate.example.com) is the IT administrator for this FortiGate unit, and the unit belongs to the Sales department located in Greenwich, London, England.

To generate a certificate request on the FortiGate unit - web-based manager:

1. Go to **System > Certificates**.
2. Select **Generate**.
3. In the **Certificate Name** field, enter `myFortiGate60`.

Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

Since the IP address is private, we will use the FQDN instead.

4. Select **Domain Name**, and enter `http://myfortigate.example.com`.
5. Enter values in the **Optional Information** area to further identify the FortiGate unit.

Organization Unit	Sales
Organization	Example.com
Locality (City)	Greenwich
State/Province	London
Country	England
e-mail	john.smith@myfortigate.example.com

6. From the **Key Type** list, select **RSA** or **Elliptic Curve**.
7. If RSA is selected, from the **Key Size** list, select **2048 Bit**. If Elliptic Curve is selected,from the **Curve Name** list, select **secp256r1**.
8. In **Enrollment Method**, select **File Based** to generate the certificate request

9. Select **OK**.
   The request is generated and displayed in the **Local Certificates** list with a status of PENDING.
10. Select the **Download** button to download the request to the management computer.
11. In the **File Download** dialog box, select ***Save*** and save the Certificate Signing Request on the local file system of the management computer.
12. Name the file and save it on the local file system of the management computer.

Example — Generate and Import CA certificate with private key pair on OpenSSL

This example explains how to generate a certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

Assumptions

Before starting this procedure, ensure that you have downloaded and installed OpenSSL on Windows. One source is: http://www.slproweb.com/products/Win32OpenSSL.html.

Generating and importing the CA certificate and private key

The two following procedures will generate a CA certificate file and private key file, and then import it to the FortiGate unit as a local certificate.

To generate the private key and certificate

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the command:
   ```
   cd c:\OpenSSL-Win32\bin
   ```
2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet123.
   ```
   openssl genrsa -des3 -out fgtcapriv.key 2048
   ```
   This command generates an RSA DES3 2048-bit encryption key.
3. The following command will generate the certificate using the key from the previous step.
   ```
   openssl req -new -x509 -days 3650 -extensions v3_ca -key fgtcapriv.key -out
       fgtca.crt
   ```
   This step generates an X509 CA certificate good for 10 years that uses the key generated in the previous step. The certificate filename is `fgtca.crt`.

   You will be prompted to enter information such as PEM Pass Phrase from the previous step, Country Name, State, Organization Name, Organizational Unit (such as department name), Common Name (the FQDN), and Email Address.

To import the certificate to the FortiGate unit - web-based manager:

1. Go to **System > Certificates**.
2. Select **Import > Local Certificate**.
3. Select **Certificate** for **Type**.
   Fields for Certificate file, Key file, and Password are displayed.
4. For **Certificate file**, enter `c:\OpenSSL-Win32\bin\fgtca.crt`.
5. For **Key file**, enter `c:\OpenSSL-Win32\bin\fgtcapriv.key`.

6. For **Password**, enter the PEM Pass Phrase you entered earlier, such as fortinet123.
7. Select **OK**.

The Certificate will be added to the list of Local Certificates and be ready for use. It will appear in the list as the filename you uploaded — `fgtca`.You can add comments to this certificate to make it clear where its from and how it is intended to be used. If you download the certificate from FortiOS, it is a .CER file.

It can now be used in Authenticating IPsec VPN users with security certificates on page 527, and Authenticating SSL VPN users with security certificates on page 526.

Optionally, you can install the certificate as a CA Certificate. CA certificates are used in HTTPS proxy/inspection. To do this, under **System > Certificates** select **Import > CA Certificate**. Select **Local PC** and enter the certificate file `c:\OpenSSL-Win32\bin\fgtca.crt`. Then select **OK**. This certificate will be displayed in the CA Certificate list under the name `CA_Cert_1`.

Example — Generate an SSL certificate in OpenSSL

This example explains how to generate a CA signed SSL certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

In this example, you will:

- Generate a CA signed SSL certificate
- Generate a self-signed SSL certificate
- Import the SSL certificate into FortiOS

Assumptions

- Before starting this procedure, ensure that you have downloaded and installed OpenSSL on MS Windows. One download source is http://www.slproweb.com/products/Win32OpenSSL.html.

Generating a CA signed SSL certificate

This procedure assumes that you have already completed Example — Generate and Import CA certificate with private key pair on OpenSSL on page 529 successfully.

To generate the CA signed SSL certificate:

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:
   ```
   cd c:\OpenSSL-Win32\bin
   ```
2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.
   ```
   openssl genrsa -des3 -out fgtssl.key 2048
   ```
   This command generates an RSA DES3 2048-bit encryption key.
3. Create a certificate signing request for the SSL certificate. This step requires you to enter the information listed in step 3 of the previous example — To generate the private key and certificate. You can leave the Challenge Password blank.
   ```
   openssl req -new -key fgtssl.key -out fgtssl.csr
   ```
4. Using the CSR from the previous step, you can now create the SSL certificate using the CA certificate that was created in Example — Generate and Import CA certificate with private key pair on OpenSSL.

```
openssl x509 -req -days 365 -in fgtssl.csr -CA fgtca.crt -CAkey fgtcapriv.key -set_
    serial 01 -out fgtssl.crt
```

This will generate an X.509 certificate good for 365 days signed by the CA certificate fgtca.crt.

Generating a self-signed SSL certificate

This procedures does not require any existing certificates.

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:
   ```
   cd c:\OpenSSL-Win32\bin
   ```
2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.
   ```
   openssl genrsa -des3 -out fgtssl.key 2048
   openssl req -new -key fgtssl.key -out fgtssl.csr
   openssl x509 -req -days 365 -in fgtssl.csr -signkey fgtssl.key -out fgtssl.crt
   ```
   These commands:
   - generate an RSA 3DES 2048-bit private key,
   - generate an SSL certificate signing request, and
   - sign the CSR to generate an SSL .CRT certificate file.

Import the SSL certificate into FortiOS

To import the certificate to FortiOS- web-based manager

1. Go to **System > Certificates**.
2. Select **Import > Local Certificate**.
3. Select **Certificate** for **Type**.
   Fields for Certificate file, Key file, and Password are displayed.
4. For **Certificate file**, enter `c:\OpenSSL-Win32\bin\fgtssl.crt`.
5. For **Key file**, enter `c:\OpenSSL-Win32\bin\fgtssl.key`.
6. For **Password**, enter the PEM Pass Phrase you entered, such as fortinet.
7. Select **OK**.

The SSL certificate you just uploaded can be found under **System > Certificates** under the name of the file you uploaded — `fgtssl`.

To confirm the certificate is uploaded properly - CLI:

```
config vpn certificate local
   edit fgtssl
      get
   end
```

The get command will display all the certificate's information. If it is not there or the information is not correct, you will need to remove the corrupted certificate (if it is there) and upload it again from your PC.

To use the new SSL certificate - CLI

```
config vpn ssl settings
   set servercert fgtssl
```

```
end
```

This assigns the fgtssl certificate as the SSL server certificate. For more information see the FortiOS Handbook SSL VPN guide.

Single Sign-On using a FortiAuthenticator unit

If you use a FortiAuthenticator unit in your network as a single sign-on agent,

- Users can authenticate through a web portal on the FortiAuthenticator unit.
- Users with FortiClient Endpoint Security installed can be automatically authenticated by the FortiAuthenticator unit through the FortiClient SSO Mobility Agent.

The FortiAuthenticator unit can integrate with external network authentication systems such as RADIUS and LDAP to gather user logon information and send it to the FortiGate unit.

User's view of FortiAuthenticator SSO authentication

There are two different ways users can authenticate through a FortiAuthenticator unit.

Users without FortiClient Endpoint Security - SSO widget

To log onto the network, the user accesses the organization's web page with a web browser. Embedded on that page is a simple logon widget, like this:

	User not logged in. Click **Login** to go to the FortiAuthenticator login page.
	User logged in. Name displayed. **Logout** button available.

The SSO widget sets a cookie on the user's browser. When the user browses to a page containing the login widget, the FortiAuthenticator unit recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login timeout expires, which can be up to 30 days.

Users with FortiClient Endpoint Security - FortiClient SSO Mobility Agent

The user simply accesses resources and all authentication is performed transparently with no request for credentials. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator unit. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The FortiClient SSO Mobility Agent, a feature of FortiClient Endpoint Security v5.0, must be configured to communicate with the appropriate FortiAuthenticator unit. After that, the agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication.

Administrator's view of FortiAuthenticator SSO authentication

You can configure either or both of these authentication types on your network.

SSO widget

You need to configure the Single Sign-On portal on the FortiAuthenticator unit. Go to **Fortinet SSO Methods > SSO > Portal Services** to do this. Copy the **Embeddable login widget** code for use on your organization's

home page. Identity-based security policies on the FortiGate unit determine which users or groups of users can access which network resources.

FortiClient SSO Mobility Agent

Your users must be running at least FortiClient Endpoint Security v5.0 to make use of this type of authentication.

On the FortiAuthenticator unit, you need to select **Enable FortiClient SSO Mobility Agent Service**, optionally select **Enable Authentication** and choose a **Secret key**. Go to **Fortinet SSO Methods > SSO > General**. You need to provide your users the FortiAuthenticator IP address and secret key so that they can configure the FortiClient SSO Mobility Agent on their computers. See Configuring the FortiGate unit on page 534.

Configuring the FortiAuthenticator unit

The FortiAuthenticator unit can poll FortiGate units, Windows Active Directory, RADIUS servers, LDAP servers, and FortiClients for information about user logon activity.

To configure FortiAuthenticator polling:

1. Go to **Fortinet SSO Methods > SSO > General**.
2. In the **FortiGate** section, leave the Listening port at 8000, unless your network requires you to change this. The FortiGate unit must allow traffic on this port to pass through the firewall.
   Optionally, you can set the Login Expiry time. This is the length of time users can remain logged in before the system logs them off automatically. The default is 480 minutes (8 hours).
3. Select **Enable Authentication** and enter the **Secret key**. Be sure to use the same secret key when configuring the FSSO Agent on FortiGate units.
4. In the **Fortinet Single Sign-On (FSSO)** section, enter

Enable Windows Active Directory domain controllers	Select for integration with Windows Active Directory.
Enable Radius accounting SSO clients	Select if you want to use a Remote Radius server.
Enable Syslog SSO	Select for integration with Syslog server.
Enable FortiClient SSO Mobility Agent service **Enable Authentication**	Select both options to enable single sign-on by clients running FortiClient Endpoint Security. Enter the **Secret key**. Be sure to use the same secret key in the FortiClient Single Sign-On Mobility Agent settings.

5. Select **OK**.

For more information, see the FortiAuthenticator Administration Guide.

Configuring the FortiGate unit

Adding a FortiAuthenticator unit as an SSO agent

On the FortiGate unit, you need to add the FortiAuthenticator unit as a Single Sign-On agent that provides user logon information.

To add a FortiAuthenticator unit as SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **Fortinet Single-Sign-On Agent**.
3. Enter a **Name** for the FortiAuthenticator unit.
4. In Primary Agent IP/Name, enter the IP address of the FortiAuthenticator unit.
5. In Password, enter the secret key that you defined for the FortiAuthenticator unit.
   On the FortiAuthenticator unit, you go to **Fortinet SSO Methods > SSO > General** to define the secret key.
   Select **Enable Authentication**.
6. Select **OK**.

In a few minutes, the FortiGate unit receives a list of user groups from the FortiAuthenticator unit. The entry in the Single Sign-On server list shows a blue caret.

When you open the server, you can see the list of groups. You can use the groups in identity-based security policies.

Configuring an FSSO user group

You cannot use FortiAuthenticator SSO user groups directly in a security policy. Create an FSSO user group and add FortiAuthenticator SSO user groups to it. FortiGate FSSO user groups are available for selection in identity-based security policies.

To create an FSSO user group:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a **Name** for the group.
3. In Type, select **Fortinet Single Sign-On (FSSO)**.
4. Add **Members**.
   The groups available to add as members are SSO groups provided by SSO agents.
5. Select **OK**.

Configuring security policies

You can create identity-based policies based on FSSO groups as you do for local user groups. For more information about security policies see the Firewall chapter.

Configuring the FortiClient SSO Mobility Agent

The user's device must have at least FortiClient Endpoint Security v5.0 installed. Only two pieces of information are required to set up the SSO Mobility Agent feature: the FortiAuthenticator unit IP address and the preshared secret.

The user needs to know the FortiAuthenticator IP address and preshared secret to set up the SSO Mobility Agent. Or, you could preconfigure FortiClient.

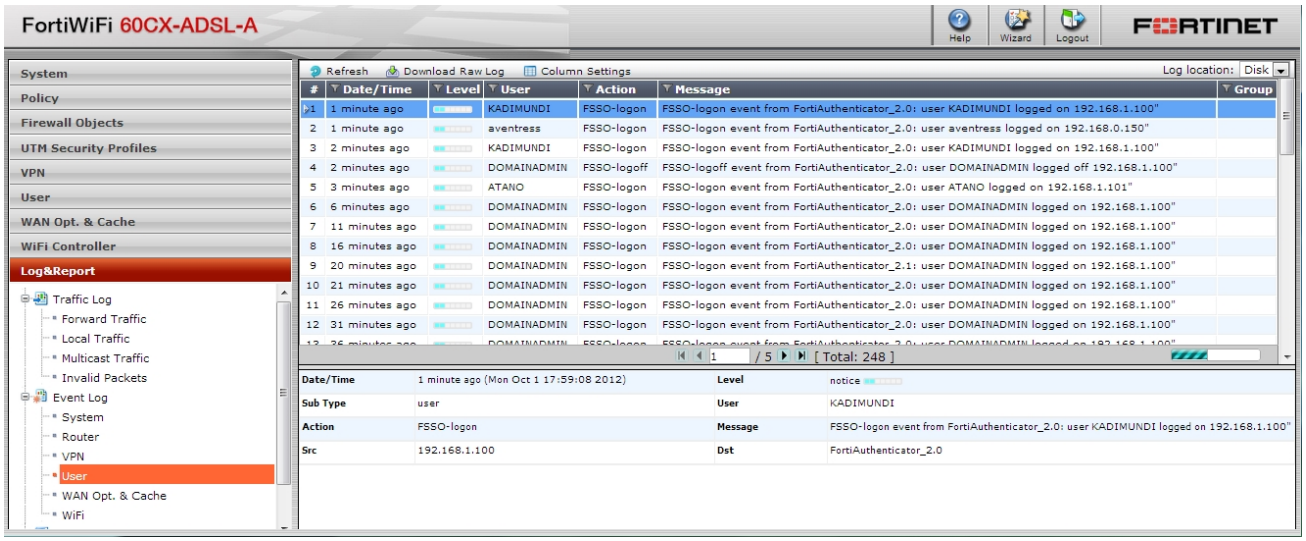
To configure FortiClient SSO Mobility Agent:

1. In FortiClient Endpoint Security, go to **File > Settings**.
   You must run the FortiClient application as an administrator to access these settings.
2. Select **Enable single sign-on mobility agent**. Enter the FortiAuthenticator unit IP address, including the listening port number specified on the FortiAuthenticator unit.
   Example: 192.168.0.99:8001. You can omit the port number if it is 8005.
3. Enter the preshared key.
4. Select **OK**.

Viewing SSO authentication events on the FortiGate unit

User authentication events are logged in the FortiGate event log.

Go to **Log & Report > Event Log > User**.



Single Sign-On to Windows AD

The FortiGate unit can authenticate users transparently and allow them network access based on their privileges in Windows AD. This means that users who have logged on to the network are not asked again for their credentials to access network resources through the FortiGate unit, hence the term “Single Sign-On”.

The following topics are included:

- Introduction to Single Sign-On with Windows AD
- Configuring Single Sign On to Windows AD
- FortiOS FSSO log messages
- Testing FSSO
- Troubleshooting FSSO

Introduction to Single Sign-On with Windows AD

Introduced in FortiOS 5.0, Single Sign-On (SSO) support provided by FortiGate polling of domain controllers is simpler than the earlier method that relies on agent software installed on Windows AD network servers. No Fortinet software needs to be installed on the Windows network. The FortiGate unit needs access only to the Windows AD global catalog and event log.

When a Windows AD user logs on at a workstation in a monitored domain, the FortiGate unit

- detects the logon event in the domain controller’s event log and records the workstation name, domain, and user,
- resolves the workstation name to an IP address,
- uses the domain controller’s LDAP server to determine which groups the user belongs to,
- creates one or more log entries on the FortiGate unit for this logon event as appropriate.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. The selection consist of matching the FSSO group or groups the user belongs to with the security policy or policies that match that group. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied.

Configuring Single Sign On to Windows AD

On the FortiGate unit, security policies control access to network resources based on user groups. With Fortinet Single Sign On, this is also true but each FortiGate user group is associated with one or more Windows AD user groups. This is how Windows AD user groups get authenticated in the FortiGate security policy.

Fortinet Single Sign On sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate unit.

To configure your FortiGate unit to operate with either a Windows AD or a Novell eDirectory FSSO install, you

- Configure LDAP access to the Windows AD global catalog. See Configuring LDAP server access on page 538.
- Configure the LDAP Server as a Single Sign-On server. See Configuring the LDAP Server as a Single Sign-On server on page 539.

- Add Active Directory user groups to FortiGate FSSO user groups. See Creating Fortinet Single Sign-On (FSSO) user groups on page 540.
- Create security policies for FSSO-authenticated groups. See Creating security policies on page 540.
- Optionally, specify a guest protection profile to allow guest access. See Enabling guest access through FSSO security policies on page 542

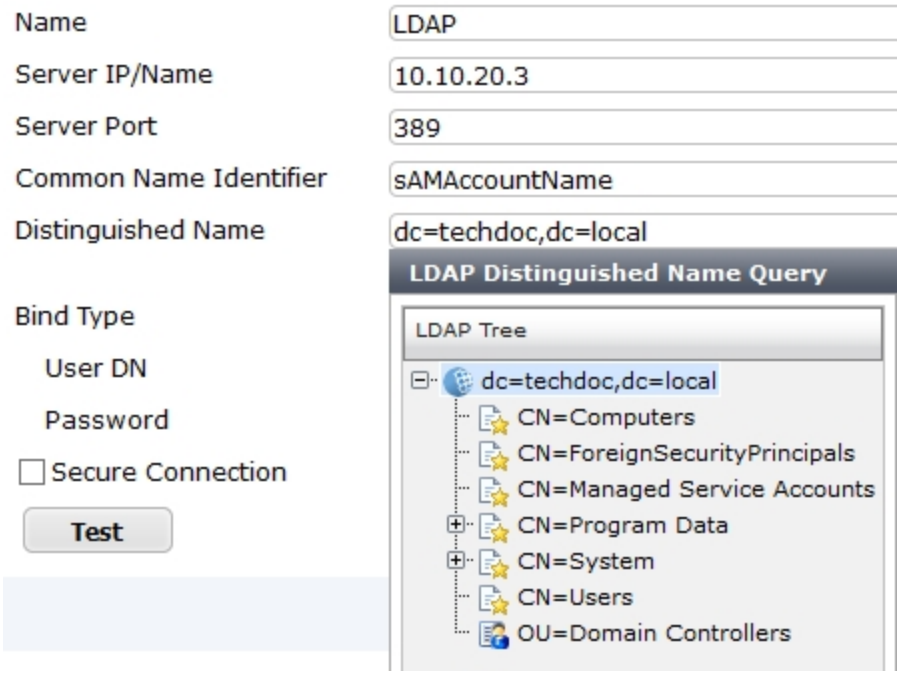
Configuring LDAP server access

The FortiGate unit needs access to the domain controller's LDAP server to retrieve user group information.

The LDAP configuration on the FortiGate unit not only provides access to the LDAP server, it sets up the retrieval of Windows AD user groups for you to select in FSSO. The LDAP Server configuration (in **User & Device > Authentication > LDAP Servers**) includes a function to preview the LDAP server's response to your distinguished name query. If you already know the appropriate Distinguished Name (DN) and User DN settings, you may be able to skip some of the following steps.

To add an LDAP server - web-based manager:

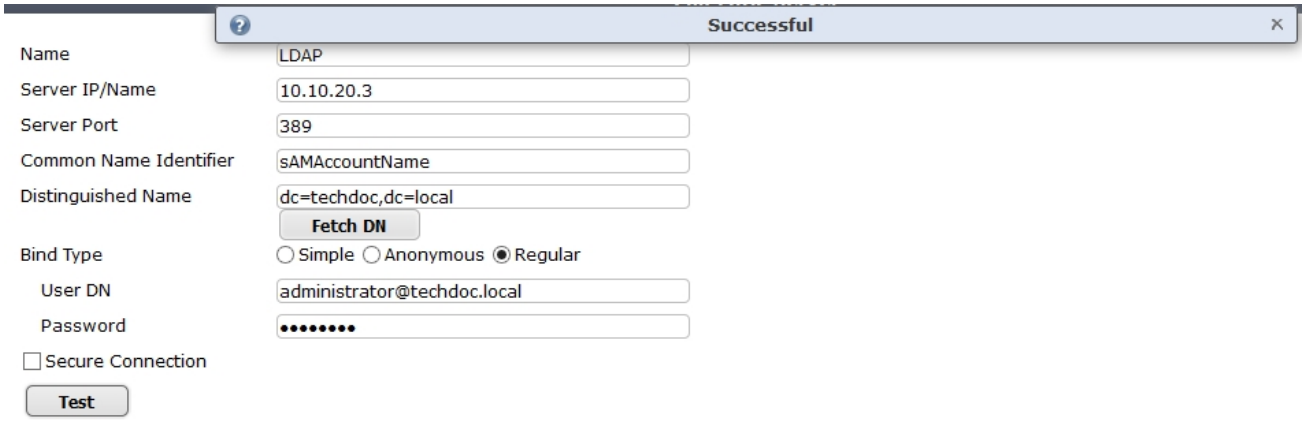
1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the **Server IP/Name** and **Server Port** (default 389).
3. In the **Common Name Identifier** field, enter **sAMAccountName**.The default common name identifier is `cn`. This is correct for most LDAP servers. However some servers use other identifiers such as `uid`.
4. In the **Distinguished Name** field, enter your organization distinguished name. In this example, Distinguished Name is dc=techdoc,dc=local
5. Select **Fetch DN**, this will fetch the Windows AD directory.



6. Set **Bind Type** to **Regular.**
7. In the **User DN** field, enter the administrative account name that you created for FSSO.
   For example, if the account is administrator, enter "administrator@techdoc.local".

8. Enter the administrative account password in the **Password** field.
9. Optionally select **Secure Connection**.
   - In the **Protocol** field, select **LDAPS** or **STARTTLS**.
   - In the **Certificate** field, select the appropriate certificate for authentication.

   Note that you need to configure the Windows AD for secure connection accordingly.
10. Select **OK**.
11. Test your configuration by selecting the **Test** button. A successful message confirming the right settings appears.



To configure LDAP for FSSO - CLI example:

```
config user ldap
   edit LDAP
      set server 10.10.20.3
      set cnid sAMAccountName
      set dn dc=techdoc,dc=local
      set type regular
      set username administrator@techdoc.local
      set password <your_password>
   next
end
```

Configuring the LDAP Server as a Single Sign-On server

The LDAP server must be added to the FortiGate Single Sign-On configuration.

To add the LDAP server as a Single Sign-On server:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. Enter

Type	Poll Active Directory Server
Server IP/Name	Server Name or IP address of the Domain Controller
User	A Domain user name
Password	The user's password

LDAP Server	Select the LDAP server you added earlier.
Enable Polling	Select

3. Select **OK**.

Creating Fortinet Single Sign-On (FSSO) user groups

You cannot use Windows or Novell groups directly in FortiGate security policies. You must create FortiGate user groups of the FSSO type and add Windows or Novell groups to them.

To create a user group for FSSO authentication - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
   The **New User Group** dialog box opens.
2. In the **Name** box, enter a name for the group, FSSO_Internet_users for example.
3. In **Type**, select **Fortinet Single Sign-On (FSSO)**.
4. In **Members**, select the required **FSSO** groups.
5. Select **OK**.

To create the FSSO_Internet-users user group - CLI

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
   end
```

Default FSSO group

`SSO_Guest_users` is a default user group enabled when FSSO is configured. It allows guest users on the network who do not have an FSSO account to authenticate and have access to network resources. See Enabling guest access through FSSO security policies on page 542.

Creating security policies

Policies that require FSSO authentication are very similar to other security policies. Using identity-based policies, you can configure access that depends on the FSSO user group. This allows each FSSO user group to have its own level of access to its own group of services

In this situation, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate

For the following procedure, the internal interface is `port1` and the external interface connected to the Internet is `port2`. There is an address group for the internal network called `company_network`. The FSSO user group is called `fsso_group`, and the FSSO RADIUS server is `fsso_rad_server`.

To configure an FSSO authentication security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IP4** and select **Create New**.
2. Enter the following information.

Incoming Interface	port1
Source Address	company_network
Source User(s)	`fsso_group`
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	HTTP, HTTPS, FTP, and Telnet
Action	ACCEPT
NAT	ON
UTM Security Profiles	ON for AntiVirus, IPS, Web Filter, and Email Filter, all using default profiles.
Log Allowed Traffic	ON. Select **Security Events**.

3. Select **OK**.
4. Ensure the FSSO authentication policy is higher in the policy list than more general policies for the same interfaces.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr company_network
      set dstaddr all
      set action accept
      set groups fsso_group
      set schedule always
      set service HTTP HTTPS FTP TELNET
      set nat enable
   end
```

Here is an example of how this FSSO authentication policy is used. Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy intercepts the session, checks with the FSSO Collector agent to verify the user's identity and credentials, and then if everything is verified the user is allowed access to the Internet.

Enabling guest access through FSSO security policies

You can enable guest users to access FSSO security policies. Guests are users who are unknown to Windows AD and servers that do not logon to a Windows AD domain.

To enable guest access in your FSSO security policy, add an identity-based policy assigned to the built-in user group `SSO_Guest_Users`. Specify the services, schedule and UTM profiles that apply to guest users — typically guests have access to a reduced set of services. See Creating security policies on page 540.

FortiOS FSSO log messages

There are two types of FortiOS log messages — firewall and event. FSSO related log messages are generated from authentication events. These include user logon and log off events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues. For more information on firewall logging, see Enabling security logging on page 498. For more information on logging, see the FortiOS Handbook Logging and Reporting guide.

Enabling authentication event logging

For the FortiGate unit to log events, that specific type of event must be enabled under logging.

When VDOMs are enabled certain options may not be available, such as CPU and memory usage events. You can enable event logs only when you are logged on to a VDOM; you cannot enable event logs globally.

To ensure you log all the events needed, set the minimum log level to Notification or Information. Firewall logging requires Notification as a minimum. The closer to Debug level, the more information will be logged.

To enable event logging:

1. Go to **Log&Report > Log Config > Log Settings**.
2. In **Event Logging**, select

System activity event	All system-related events, such as ping server failure and gateway status.
User activity event	All administration events, such as user logins, resets, and configuration updates.

3. Select **Apply**.

List of FSSO related log messages

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication was successful

Message ID	Severity	Description
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication was successful
43017	Notification	NTLM authentication failed

For more information on logging, see the FortiOS Handbook Logging and Reporting guide.

Testing FSSO

Once FSSO is configured, you can easily test to ensure your configuration is working as expected. For additional FSSO testing, see Troubleshooting FSSO on page 543.

1. Logon to one of the stations on the FSSO domain, and access an Internet resource.
2. Connect to the CLI of the FortiGate unit, and if possible log the output.
3. Enter the following command:`diagnose debug authd fsso list`
4. Check the output. If FSSO is functioning properly you will see something similar to the following:

```
----FSSO logons----
IP: 192.168.1.230 User: ADMINISTRATOR Groups: VLAD-AD/DOMAIN USERS
IP: 192.168.1.240 User: ADMINISTRATOR Groups: VLAD-AD/DOMAIN USERS
Total number of users logged on: 2
----end of FSSO logons----
```

   The exact information will vary based on your installation.

5. Check the FortiGate event log, for FSSO-auth action or other FSSO related events with FSSO information in the message field.
6. To check server connectivity, run the following commands from the CLI:

```
FGT# diagnose debug enable
FGT# diagnose debug authd fsso server-status
FGT# Server Name Connection Status
     ----------- -----------------
     SBS-2003 connected
```

Troubleshooting FSSO

When installing, configuring, and working with FSSO some problems are quite common. A selection of these problems follows including explanations and solutions.

Some common Windows AD problems include:

- General troubleshooting tips for FSSO
- Users on a particular computer (IP address) can not access the network
- Guest users do not have access to network

General troubleshooting tips for FSSO

The following tips are useful in many FSSO troubleshooting situations.

- Ensure all firewalls are allowing the FSSO required ports through.
  FSSO has a number of required ports that must be allowed through all firewalls or connections will fail. These include: ports 139, 389 (LDAP), 445, 636 (LDAP).
- Ensure there is at least 64kbps bandwidth between the FortiGate unit and domain controllers. If there is insufficient bandwidth, some FSSO information might not reach the FortiGate unit. The best solution is to configure traffic shaping between the FortiGate unit and the domain controllers to ensure that the minimum bandwidth is always available.

Users on a particular computer (IP address) can not access the network

Windows AD Domain Controller agent gets the username and workstation where the logon attempt is coming from. If there are two computers with the same IP address and the same user trying to logon, it is possible for the authentication system to become confused and believe that the user on computer_1 is actually trying to access computer_2.

Windows AD does not track when a user logs out. It is possible that a user logs out on one computer, and immediate logs onto a second computer while the system still believes the user is logged on the original computer. While this is allowed, information that is intended for the session on one computer may mistakenly end up going to the other computer instead. The result would look similar to a hijacked session.

Solutions

- Ensure each computer has separate IP addresses.
- Encourage users to logout on one machine before logging onto another machine.
- If multiple users have the same username, change the usernames to be unique.
- Shorten timeout timer to flush inactive sessions after a shorter time.

Guest users do not have access to network

A group of guest users was created, but they don’t have access.

Solution

The group of the guest users was not included in a policy, so they do not fall under the guest account. To give them access, associate their group with a security policy.

Additionally, there is a default group called `SSO_Guest_Users`. Ensure that group is part of an identity-based security policy to allow traffic.

Agent-based FSSO

FortiOS can provide single sign-on capabilities to Windows AD, Citrix, or Novell eDirectory users with the help of agent software installed on these networks. The agent software sends information about user logons to the FortiGate unit. With user information such as IP address and user group memberships from the network, FortiGate security policies can allow authenticated network access to users who belong to the appropriate user groups without requesting their credentials again.

For Windows AD networks, FortiGate units can provide SSO capability without agent software by directly polling the Windows AD domain controllers. For information about this type of SSO, seeSingle Sign-On to Windows AD on page 537.

The following topics are included:

- Introduction to agent-based FSSO
- FSSO NTLM authentication support
- Agent installation
- Configuring the FSSO Collector agent for Windows AD
- Configuring the FSSO TS agent for Citrix
- Configuring FSSO with Novell networks
- Configuring FSSO Advanced Settings
- Configuring FSSO on FortiGate units
- FortiOS FSSO log messages
- Testing FSSO
- Troubleshooting FSSO

Introduction to agent-based FSSO

Fortinet Single Sign-On (FSSO), through agents installed on the network, monitors user logons and passes that information to the FortiGate unit. When a user logs on at a workstation in a monitored domain, FSSO

- detects the logon event and records the workstation name, domain, and user,
- resolves the workstation name to an IP address,
- determines which user groups the user belongs to,
- sends the user logon information, including IP address and groups list, to the FortiGate unit
- creates one or more log entries on the FortiGate unit for this logon event as appropriate.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied.

FSSO can also provide NTLM authentication service for requests coming from FortiGate. SSO is very convenient for users, but may not be supported across all platforms. NTLM is not as convenient, but it enjoys wider support. See FSSO NTLM authentication support on page 551.

Introduction to FSSO agents

There are several different FSSO agents that can be used in an FSSO implementation:

- Domain Controller (DC) agent
- eDirectory agent
- Citrix/Terminal Server (TS) agent
- Collector (CA) agent

Consult the latest FortiOS and FSSO Release Notes for operating system compatibility information.

Domain Controller (DC) agent

The Domain Controller (DC) agent must be installed on every domain controller if you will use DC Agent mode, but is not required if you use Polling mode. See FSSO for Windows AD on page 547.

eDirectory agent

The eDirectory agent is installed on a Novell network to monitor user logons and send the required information to the FortiGate unit. It functions much like the Collector agent on a Windows AD domain controller.The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.

Citrix/Terminal Server (TS) agent

The Citrix/Terminal Server (TS) agent is installed on a Citrix terminal server to monitor user logons in real time. It functions much like the DC Agent on a Windows AD domain controller.

Collector (CA) agent

This agent is installed as a service on a server in the Windows AD network to monitor user logons and send the required information to the FortiGate unit. The Collector agent can collect information from

- Domain Controller agent (Windows AD)
- TS agent (Citrix Terminal Server)

In a Windows AD network, the Collector agent can optionally obtain logon information by polling the AD domain controllers. In this case, DC agents are not needed.

The Collector can obtain user group information from the DC agent or optionally, a FortiGate unit can obtain group information directly from AD using Lightweight Directory Access Protocol (LDAP).

On a Windows AD network, the FSSO software can also serve NT LAN Manager (NTLM) requests coming from client browsers (forwarded by the FortiGate unit) with only one or more Collector agents installed. See FSSO NTLM authentication support on page 551.

The CA is responsible for DNS lookups, group verification, workstation checks, and as mentioned FortiGate updates of logon records. The FSSO Collector Agent sends Domain Local Security Group and Global Security Group information to FortiGate units. The CA communicates with the FortiGate over TCP port 8000 and it listens on UDP port 8002 for updates from the DC agents.

The FortiGate unit can have up to five CAs configured for redundancy. If the first on the list is unreachable, the next is attempted, and so on down the list until one is contacted. See Configuring FSSO on FortiGate units on page 579.

All DC agents must point to the correct Collector agent port number and IP address on domains with multiple DCs.

A FortiAuthenticator unit can act much like a Collector agent, collecting Windows AD user logon information and sending it to the FortiGate unit. It is particularly useful in large installations with several FortiGate units. For more information, see the FortiAuthenticator Administration Guide.

FSSO for Windows AD

FSSO for Windows AD requires at least one Collector agent. Domain Controller agents may also be required depending on the Collector agent working mode. There are two working modes to monitor user logon activity: DC Agent mode or Polling mode.

Collector agent DC Agent mode versus Polling mode

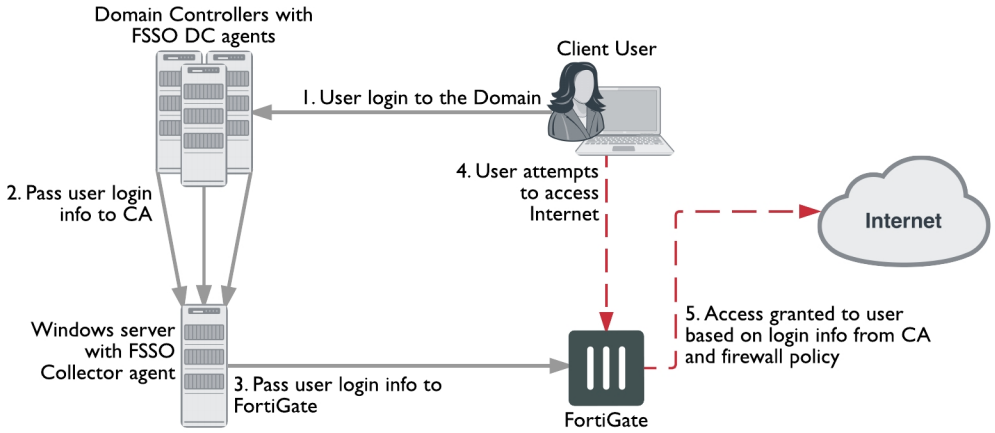
	DC Agent mode	Polling Mode
Installation	Complex — Multiple installations: one agent per DC plus Collector agent, requires a reboot	Easy — Only Collector agent installation, no reboot required
Resources	Shares resources with DC system	Has own resources
Network load	Each DC agent requires minimum 64kpbs bandwidth, adding to network load	Increase polling period during busy period to reduce network load
Level of Confidence	Captures all logons	Potential to miss a login if polling period is too great

DC Agent mode

DC Agent mode is the standard mode for FSSO. In DC Agent mode, a Fortinet authentication agent is installed on each domain controller. These DC agents monitor user logon events and pass the information to the Collector agent, which stores the information and sends it to the FortiGate unit.

The DC agent installed on the domain controllers is not a service like the Collector agent — it is a DLL file called `dcagent.dll` and is installed in the `Windows\system32` directory. It must be installed on all domain controllers of the domains that are being monitored.

FSSO in DC agent mode



DC Agent mode provides reliable user logon information, however you must install a DC agent on every domain controller. A reboot is needed after the agent is installed. Each installation requires some maintenance as well. For these reasons it may not be possible to use the DC Agent mode.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality. You can optionally configure traffic shapers on the FortiGate unit to ensure this minimum bandwidth is guaranteed for the domain controller connections.

Polling mode

In Polling mode there are three options — NetAPI polling, Event log polling, and Event log using WMI. All share the advantages of being transparent and agentless.

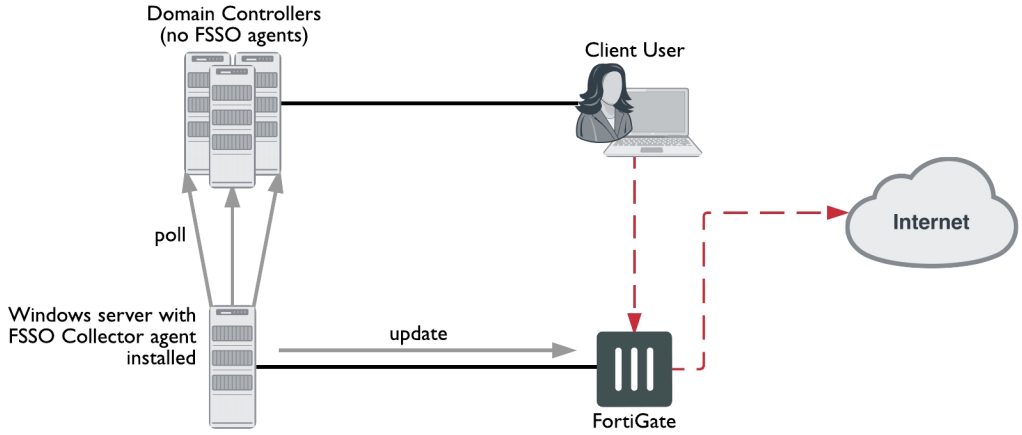
NetAPI polling is used to retrieve server logon sessions. This includes the logon event information for the Controller agent. NetAPI runs faster than Event log polling but it may miss some user logon events under heavy system load. It requires a query round trip time of less than 10 seconds.

Event log polling may run a bit slower, but will not miss events, even when the installation site has many users that require authentication. It does not have the 10 second limit on NetAPI polling. Event log polling requires fast network links. Event log polling is required if there are Mac OS users logging into Windows AD.

Event log using WMI polling: WMI is a Windows API to get system information from a Windows server, CA is a WMI client and sends WMI queries for user logon events to DC, which in this case is a WMI server. Main advantage in this mode is that CA does not need to search security event logs on DC for user logon events, instead, DC returns all requested logon events via WMI. This also reduces network load between CA and DC.

In Polling mode, the Collector agent polls port 445 of each domain controller for user logon information every few seconds and forwards it to the FortiGate unit. There are no DC Agents installed, so the Collector agent polls the domain controllers directly.

FSSO in Polling mode



A major benefit of Polling mode is that no FSSO DC Agents are required. If it is not possible to install FSSO DC Agents on your domain controllers, this is the alternate configuration available to you. Polling mode results in a less complex install, and reduces ongoing maintenance. The minimum permissions required in Polling mode are to read the event log or call NetAPI.

Collector agent AD Access mode - Standard versus Advanced

The Collector agent has two ways to access Active Directory user information. The main difference between Standard and Advanced mode is the naming convention used when referring to username information.

Standard mode uses regular Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

If there is no special requirement to use LDAP— best practices suggest you set up FSSO in Standard mode. This mode is easier to set up, and is usually easier to maintain and troubleshoot.

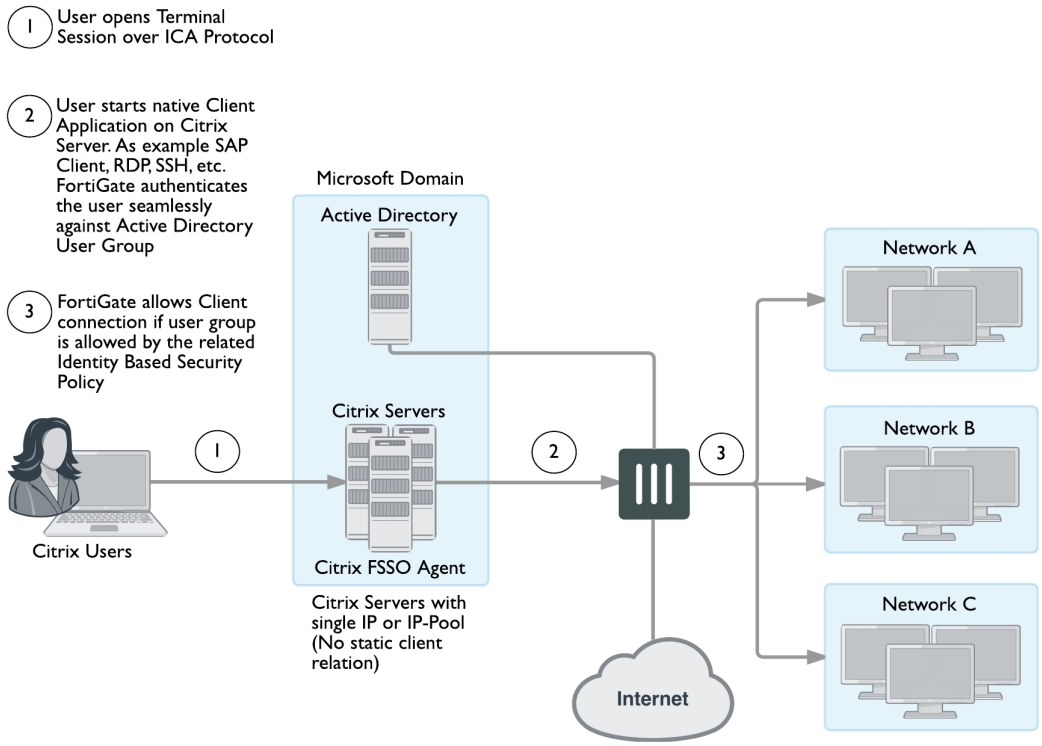
Standard and advanced modes have the same level of functionality with the following exceptions:

- Users have to create Group filters on the Collector agent. This differs from Advanced mode where Group filters are configured from the FortiGate unit. Fortinet strongly encourages users to create filters from CA.
- Advanced mode supports nested or inherited groups. This means that users may be a member of multiple monitored groups. Standard mode does not support nested groups so a user must be a direct member of the group being monitored.

FSSO for Citrix

Citrix users can enjoy a similar Single Sign-On experience as Windows AD users. The FSSO TS agent installed on each Citrix server provides user logon information to the FSSO Collector agent on the network. The FortiGate unit uses this information to authenticate the user in security policies.

Citrix SSO topology



Citrix users do not have unique IP addresses. When a Citrix user logs on, the TS agent assigns that user a range of ports. By default each user has a range of 200 ports.

FSSO for Novell eDirectory

FSSO in a Novell eDirectory environment works similar to the FSSO Polling mode in the Windows AD environment. The eDirectory agent polls the eDirectory servers for user logon information and forwards the information to the FortiGate unit. There is no need for the Collector agent.

When a user logs on at a workstation, FSSO:

- detects the logon event by polling the eDirectory server and records the IP address and user ID,
- looks up in the eDirectory which groups this user belongs to,
- sends the IP address and user groups information to the FortiGate unit.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is supported on the Novell E-Directory 8.8 operating system.

For a Novell network, there is only one FSSO component to install — the eDirectory agent. In some cases, you also need to install the Novell Client.

FSSO security issues

When the different components of FSSO are communicating there are some inherent security features.

FSSO installation requires an account with network admin privileges. The security inherent in these types of accounts helps ensure access to FSSO configurations is not tampered with.

User passwords are never sent between FSSO components. The information that is sent is information to identify a user including the username, group or groups, and IP address.

NTLM uses base-64 encoded packets, and uses a unique randomly generated challenge nonce to avoid sending user information and password between the client and the server.

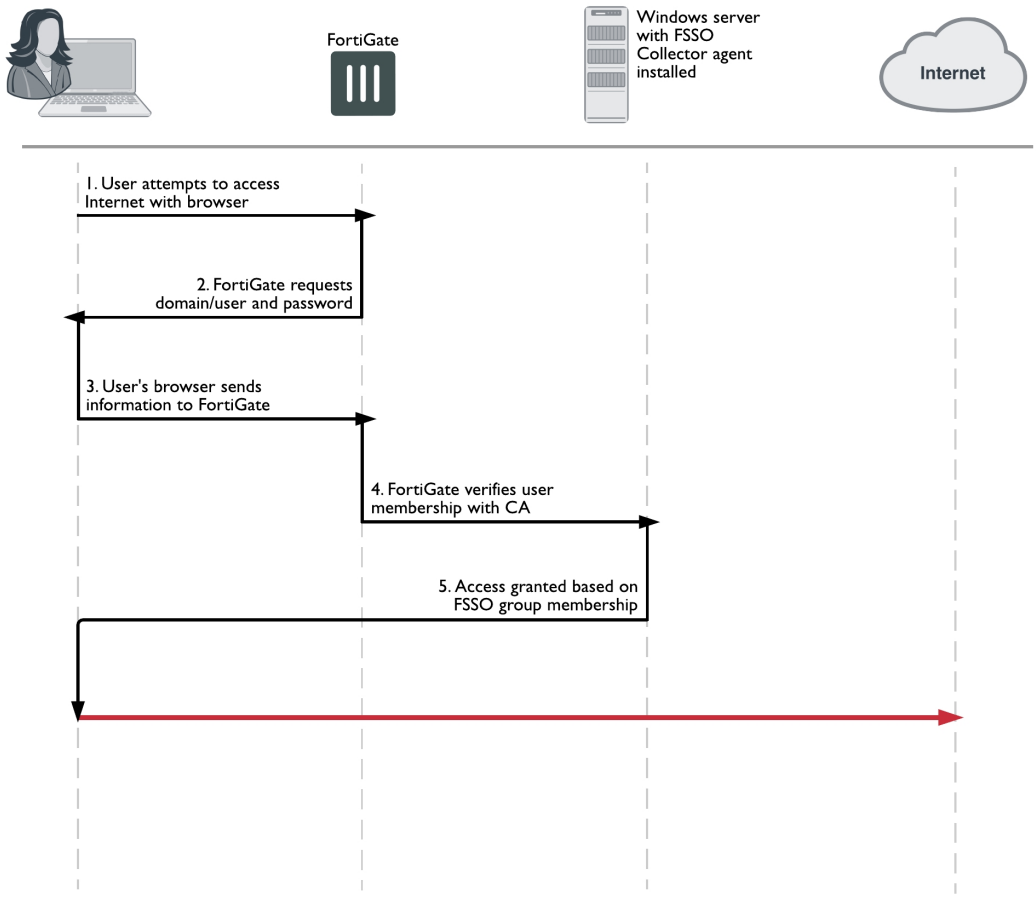
FSSO NTLM authentication support

In a Windows AD network, FSSO can also provide NTLM authentication service to the FortiGate unit. When the user makes a request that requires authentication, the FortiGate unit initiates NTLM negotiation with the client browser. The FortiGate unit does not process the NTLM packets itself. Instead, it forwards all the NTLM packets to the FSSO service to process.

NTLM has the benefit of not requiring an FSSO agent, but it is not transparent to users, and the user's web browser must support NTLM.

The NTLM protocol protects the user's password by not sending it over the network. Instead, the server sends the client a random number that the client must encrypt with the hash value of the user's password. The server compares the result of the client's encryption with the result of its own encryption. The two will match only if both parties used the same password.

NTLM authentication



If the NTLM authentication with the Windows AD network is successful, and the user belongs to one of the groups permitted in the applicable security policy, the FortiGate unit allows the connection but will require authentication again in the future when the current authentication expires.

Fortinet has tested NTLM authentication with Internet Explorer and Firefox browsers.

NTLM in a multiple domain environment

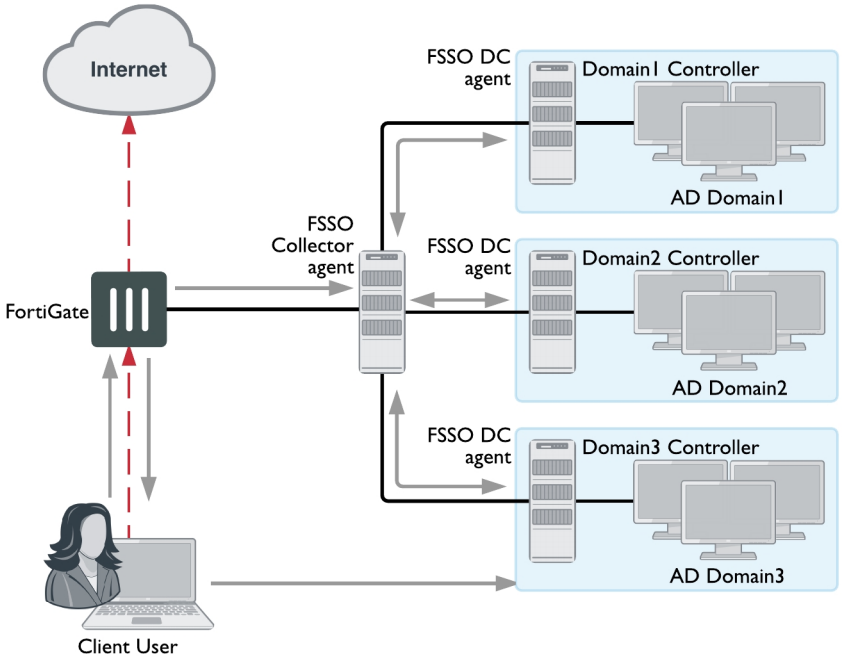
In a multiple domain environment for NTLM, the important factor is that there is a trust relation between the domains. In a forest, this relation is automatically created. So you can install FSSO agent on one of the domain controllers without worry.

But in case of multiple domains that are not in a forest, you need to create a trust relation between the domains. If you do not want to have a trust relation between your multiple domains, you need to use FSAE 4.0 MR1 and the DC agent needs to be installed once on each domain. Then you can use security policies to configure server access.

In the figure below, three domains are shown connected to the FSSO Collector agent server. The Client logs on to their local Domain Controller, which then sends the user logon event information to the Collector Agent. When the Client attempts to access the Internet, the FortiGate unit contacts the Collector Agent for the logon information, sees the Client is authenticated, and allows access to the Internet. There are multiple domains each

with a domain controller agent (DCagent) that sends logon information to the Collector agent. If the multiple domains have a trust relationship, only one DCagent is required instead of one per domain.

FSSO NTLM with multiple domains not in a forest



Understanding the NTLM authentication process

1. The user attempts to connect to an external (internet) HTTP resource. The client application (browser) on the user's computer issues an unauthenticated request through the FortiGate unit.
2. The FortiGate is aware that this client has not authenticated previously, so responds with a `401 Unauthenticated` status code, and tells the client which authentication method to reply with in the header: `Proxy-Authenticated: NTLM`. Then the initial session is dismantled.
3. The client application connects again to the FortiGate, and issues a GET-request, with a `Proxy-Authorization: NTLM <negotiate string>` header. `<negotiate-string>` is a base64-encoded NTLM Type 1 negotiation packet.
4. The FortiGate unit replies with a `401 "proxy auth required"` status code, and a `Proxy-Authenticate: NTLM <challenge string>` (a base 64-encoded NTLM Type 2 challenge packet). In this packet is the challenge nonce, a random number chosen for this negotiation that is used once and prevents replay attacks.

The TCP connection must be kept alive, as all subsequent authentication-related information is tied to the TCP connection. If it is dropped, the authentication process must start again from the beginning.

5. The client sends a new GET-request with a header: `Proxy-Authenticate: NTLM <authenticate string>`, where `<authenticate string>` is a NTLM Type 3 Authentication packet that contains:

- username and domain
- the challenge nonce encoded with the client password (it may contain the challenge nonce twice using different algorithms).

6. If the negotiation is successful and the user belongs to one of the groups permitted in the security policy, the connection is allowed, Otherwise, the FortiGate unit denies the authentication by issuing a 401 return code and prompts for a username and password. Unless the TCP connection is broken, no further credentials are sent from the client to the proxy.

If the authentication policy reaches the authentication timeout period, a new NTLM handshake occurs.

Agent installation

After reading the appropriate sections of Introduction to agent-based FSSO on page 545 to determine which FSSO agents you need, you can proceed to perform the necessary installations.

Ensure you have administrative rights on the servers where you are installing FSSO agents. It is best practice to install FSSO agents using the built-in local administrator account. Optionally, you can install FSSO without an admin account. See Installing FSSO without using an administrator account on page 556.

In Windows 2008 by default, you do not have administrative user rights if you are logged on as a user other than as the built-in administrator, even if you were added to the local Administrators group on the computer.

The FSSO installer first installs the Collector agent. You can then continue with installation of the DC agent, or you can install it later by going to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**. The installer will install a DC agent on the domain controllers of all of the trusted domains in your network.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality.Traffic shapers configured on the FortiGate can help guarantee these minimum bandwidths.

Collector agent installation

To install FSSO, you must obtain the FSSO_Setup file from the Fortinet Support web site. This is available as either an executable (.exe) or a Microsoft Installer (.msi) file. Then you follow these two installation procedures on the server that will run the Collector agent. This can be any server or domain controller that is part of your network. These procedures also installs the DC Agent on all of the domain controllers in your network.

To install the Collector agent:

1. Create an account with administrator privileges and a password that does not expire. See Microsoft Advanced Server documentation for help with this task.
   To use a non-admin read only account, see Installing FSSO without using an administrator account on page 556.
2. Log on to the account that you created in Step 1.
3. Double-click the `FSSOSetup.exe` file.
   The Fortinet SSO Collector Agent Setup Wizard starts.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, you can change the installation location. Select **Next**.
7. Optionally, change the **User Name**.
8. By default, the agent is installed using the currently running account. If you want FSSO to use another existing admin account, change the **User Name** using the format DomainName \ UserName. For example if the account is `jsmith` and the domain is **example_corp** you would enter `example_corp\jsmith`.
9. In the **Password** field, enter the password for the account listed in the **User Name** field.
10. Select **Next**.
11. Enable as needed:
    - Monitor user logon events and send the information to the FortiGate unit
    - Serve NTLM authentication requests coming from FortiGate
      By default, both methods are enabled. You can change these options after installation.
12. Select the access method to use for Windows Directory:
13. Select **Standard** to use Windows domain and username credentials.
14. Select **Advanced** if you will set up LDAP access to Windows Directory.
    See Collector agent AD Access mode - Standard versus Advanced on page 549.
15. Select **Next** and then select **Install**.
    If you want to use DC Agent mode, ensure that **Launch DC Agent Install Wizard** is selected. This will start DC agent installation immediately after you select **Finish**.
16. Select **Finish**.

If you see an error such as Service Fortinet Single Sign On agent (service_FSAE) failed to start, there are two possible reasons for this. Verify the user account you selected has sufficient privileges to run the FSSO service. Also verify the computer system you are attempting to install on is a supported operating system and version.

DC agent installation

The FSSO_Setup file contains both the Collector agent and DC Agent installers, but the DC Agent installer is also available separately as either a .exe or .msi file named DCAgent_Setup.

To install the DC Agent

1. If you have just installed the Collector agent, the FSSO - Install DC Agent wizard starts automatically. Otherwise, go to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**.
2. Select **Next**.
3. Read and accept the license agreement. Select **Next**.

4. Optionally, you can change the installation location. Select **Next**.
5. Enter the **Collector agent IP address**.
6. If the Collector agent computer has multiple network interfaces, ensure that the one that is listed is on your network. The listed **Collector agent listening port** is the default. Only change this if the port is already used by another service.
7. Select **Next**.
8. Select the domains to monitor and select **Next**.
9. If any of your required domains are not listed, cancel the wizard and set up the proper trusted relationship with the domain controller. Then run the wizard again by going to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**.
10. Optionally, select users that you do not want monitored. These users will not be able to authenticate to FortiGate units using FSSO. You can also do this later. See Configuring the FSSO Collector agent for Windows AD on page 560.
11. Select **Next**.
12. Optionally, clear the check boxes of domain controllers on which you do not want to install the DC Agent.
13. Select the **Working Mode** as DC Agent Mode. While you can select Polling Mode here, in that situation you would not be installing a DC Agent. For more information, see DC Agent mode on page 547 and Polling mode on page 548.
14. Select **Next**.
15. Select **Yes** when the wizard requests that you reboot the computer.

If you reinstall the FSSO software on this computer, your FSSO configuration is replaced with default settings.

If you want to create a redundant configuration, repeat the Collector agent installation procedure on at least one other Windows AD server.

When you start to install a second Collector agent, cancel the Install Wizard dialog appears the second time. From the configuration GUI, the monitored domain controller list will show your domain controllers un-selected. Select the ones you wish to monitor with this Collector agent, and select **Apply**.

Before you can use FSSO, you need to configure it on both Windows AD and on the FortiGate units. Configuring FSSO on FortiGate units on page 579 will help you accomplish these two tasks.

Installing FSSO without using an administrator account

Normally when installing services in Windows, it is best to use the Domain Admin account, as stated earlier. This ensures installation goes smoothly and uninterrupted, and when using the FSSO agent there will be no permissions issues. However, it is possible to install FSSO with a non-admin account in Windows 2003 or 2008 AD.

The following instructions for Windows 2003 are specific to the event log polling mode only. Do not use this procedure with other FSSO configurations.

Windows 2003

There are two methods in Windows 2003 AD for installing FSSO without an admin account — add the non-admin user to the security log list, and use a non-admin account with read-only permissions. A problem with the first method is that full rights (read, write, and clear) are provided to the event log. This can be a problem when audits require limited or no write access to logs. In those situations, the non-admin account with read-only permissions is the solution.

To add the non-admin user account to the Windows 2003 security log list :

1. Go to **Default Domain Controller Security Settings > Security Settings > User Rights Assignment > Manage auditing and security log**.
2. Add the user account to this list.
3. Repeat these steps on every domain controller in Windows 2003 AD.
   A reboot is required.

To use a non-admin account with read-only permissions to install FSSO on Windows 2003:

The following procedure provides the user account specified with read only access to the Windows 2003 AD Domain Controller Security Event Log which allows FSSO to function.

1. Find out the SID of the account you intend to use.
   Tools for this can be downloaded for free from http://technet.microsoft.com/en-us/sysinternals/bb897417.
2. Then create the permission string. For example:
   - `(A;;0x1;;;S-1-5-21-4136056096-764329382-1249792191-1107)`
   - `A` means Allow,
   - `0x1` means Read, and
   - `S-1-5-21-4136056096-764329382-1249792191-1107` is the SID.
3. Then, append it to the registry key:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Security\CustomSD`
4. Repeat these steps on every domain controller in Windows 2003 AD.
   A reboot is required.

Windows 2008

In Windows 2008 AD, if you do not want to use the Domain Admin account then the user account that starts the FSSO agent needs to be added to the Event Log Readers group.

When the user is added to the Event Log Readers group, that user is now allowed to have read only access to the event log and this is the minimal rights required for FSSO to work.

Citrix TS agent installation

To install the Citrix TS agent, you must obtain the TSAgent_Setup file from the Fortinet Support web site. Perform the following installation procedure on the Citrix server.

To install the FSSO TS agent:

1. On the Citrix server, create an account with administrator privileges and a password that does not expire. See Citrix documentation for more information.

2. Log on to the account that you created in step 1.
3. Double-click the TSAgent_Setup installation file.
   The Fortinet SSO Terminal Server Agent Setup Wizard starts.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, you can change the installation location. Select **Next**.
7. Verify that **This Host IP Address** is correct.
8. In the **FSSO Collector Agent List**, enter the IP address(es) of your Collector Agents.
9. Select **Next** and then select **Install**.
   The TS agent is installed.
10. Select **Finish**.

Novell eDirectory agent installation

To install the eDirectory agent, you must obtain the FSSO_Setup_eDirectory file from the Fortinet Support web site. Perform the following installation procedure on the computer that will run the eDirectory agent. This can be any server or domain controller that is part of your network. You will need to provide some setup information.

To install the FSSO eDirectory agent:

1. Create an account with administrator privileges and a password that does not expire. See Novell documentation for more information.
2. Log on to the account that you created in step 1.
3. Double-click the FSSO_Setup_edirectory file to start the installation wizard.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, change the installation location. Select **Next**.
7. Enter:

eDirectory Server	
Server Address	Enter the IP address of the eDirectory server.
Use secure connection (SSL)	Select to connect to the eDirectory server using SSL security.
Search Base DN	Enter the base Distinguished Name for the user search.

eDirectory Authentication	
Username	Enter a username that has access to the eDirectory, using LDAP format.
User password	Enter the password.

8. Select **Next**.
9. Select **Install**. When the installation completes, select **Finish**.

Updating FSSO agents on Windows AD

After FSSO is installed on your network, you may want to upgrade to a newer version. The following procedure helps ensure you have a trouble free upgrade. How you update FSSO depends on if you are using polling mode or DCAgent mode.

For polling mode, since there are no DC agents you only need to upgrade the Collector. However in DCAgent mode, each DC Agent must be updated as well.

To update FSSO in DC Agent mode:

1. Go to the system32 directory on all DC's and rename the `dcagent.dll` file to `dcagent.dll.old`.
   This ensures the when the upgrade is pushed to the DC it does not overwrite the old file. If there are any problems this makes it easy to revert to the old version.
2. Run the FSSO setup .exe file to update the collector. When this is completed, ignore any reboot message.
3. Go to **Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent** and push the DC agent out to all servers. All DC's will now need to be rebooted so that the new DLL file is loaded.
4. After the reboot, go to all DC's and delete the `dcagent.dll.old` files.

Configuring the FSSO Collector agent for Windows AD

On the FortiGate unit, security policies control access to network resources based on user groups. With Fortinet Single Sign On, this is also true but each FortiGate user group is associated with one or more Windows AD user groups. This is how Windows AD user groups get authenticated in the FortiGate security policy.

Fortinet Single Sign On sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units.

To avoid this problem, you can configure the Fortinet Single Sign On Collector agent to send logon information only for groups named in the FortiGate unit's security policies. See Configuring FortiGate group filters on page 567.

On each server with a Collector agent, you will be

- Configuring Windows AD server user groups
- Configuring Collector agent settings, including the domain controllers to be monitored
- Selecting Domain Controllers and working mode for monitoring
- Configuring Directory Access settings
- Configuring the Ignore User List
- Configuring FortiGate group filters for each FortiGate unit
- Configuring FSSO ports
- Configuring alternate user IP address tracking
- Viewing FSSO component status

Configuring Windows AD server user groups

FortiGate units control network resource access at the group level. All members of a user group have the same network access as defined in FortiGate security policies.

You can use existing Windows AD user groups for authentication to FortiGate units if you intend that all members within each group have the same network access privileges.

Otherwise, you need to create new user groups for this purpose.

If you change a user's group membership, the change does not take effect until the user logs off and then logs on again.

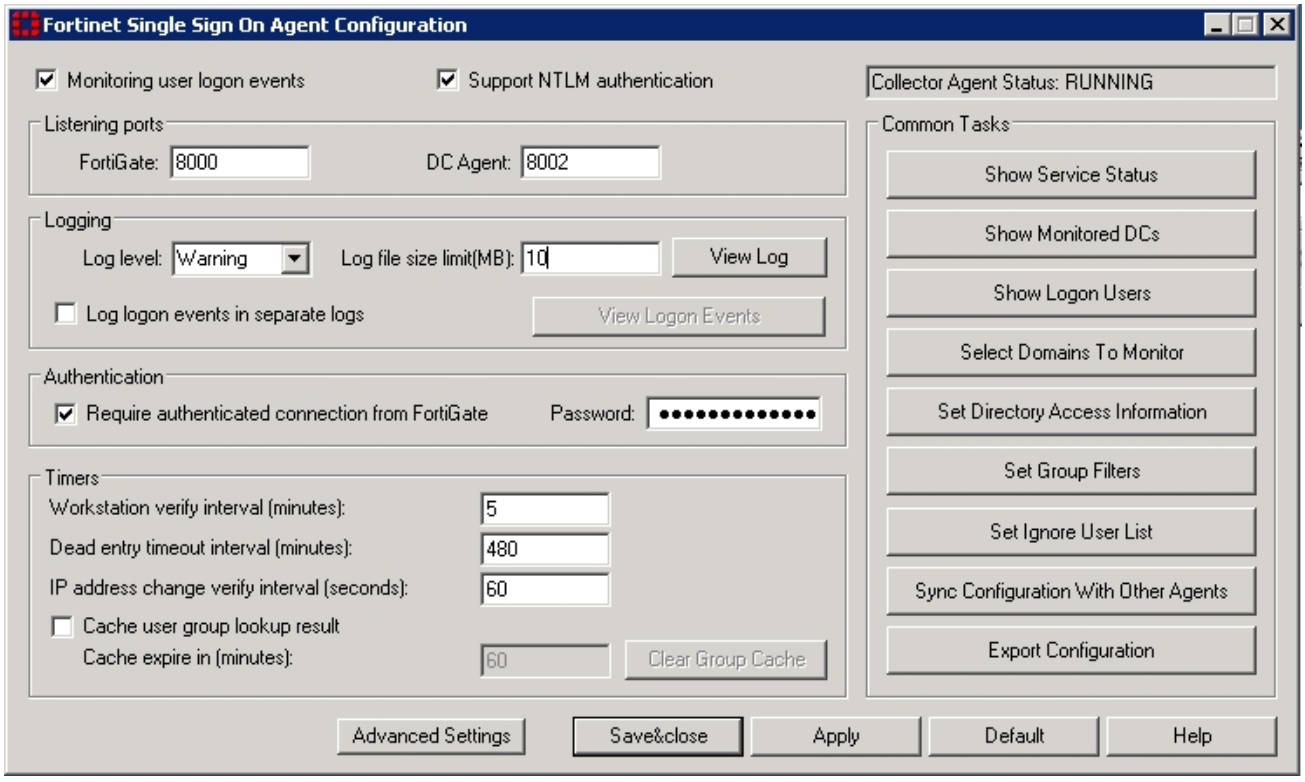
The FSSO Agent sends only Domain Local Security Group and Global Security Group information to FortiGate units. You cannot use Distribution group types for FortiGate access. No information is sent for empty groups.

Refer to Microsoft documentation for information about creating and managing Windows AD user groups.

Configuring Collector agent settings

You need to configure which domain controllers the Collector agent will use and which domains to monitor for user logons. You can also alter default settings and settings you made during installation. These tasks are accomplished by configuring the FSSO Collector Agent, and selecting either Apply to enable the changes.

At any time to refresh the FSSO Agent settings, select Apply.



To configure the Collector agent:

1. From the Start menu, select **Programs > Fortinet > Fortinet Single Sign-On Agent > Configure Fortinet Single Sign-On Agent**.
2. Enter the following information.

Monitoring user logon events	By default, this is enabled to automatically authenticate users as they log on to the Windows domain. Disable the Monitor feature only if you have a large network where this feature will slow responses too much.
Support NTLM authentication	By default, this is enabled to facilitate logon of users who are connected to a domain that does not have the FSSO DC Agent installed. Disable NTLM authentication only if your network does not support NTLM authentication for security or other reasons.
Collector Agent Status	Shows RUNNING when Collector agent is active.

Listening ports		You can change FSSO Collector Agent related port numbers if necessary.
	FortiGate	TCP port for FortiGate units. Default 8000.
	DC Agent	UDP port for DC Agents. Default 8002.
Logging		
	Log level	Select the minimum severity level of logged messages.
	Log file size limit (MB)	Enter the maximum size for the log file in MB. Default is 10.
	View Log	View all Fortinet Single Sign On agent logs.
	Log logon events in separate logs	Record user login-related information separately from other logs. The information in this log includes: • data received from DC agents • user logon/logoff information • workstation IP change information • data sent to FortiGate units
	View Logon Events	If **Log logon events in separate logs** is enabled, you can view user login-related information.
Authentication		
	Require authenticated connection from FortiGate	Select to require the FortiGate unit to authenticate before connecting to the Collector agent.
	Password	Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “fortinetcanada”. It is highly recommended to modify this password.
Timers		
	Workstation verify interval (minutes)	Enter the interval in minutes at which the Fortinet Single Sign On Collector agent connects to client computers to determine whether the user is still logged on. The default is every 5 minutes. The interval may be increased if your network has too much traffic. **Note:** This verification process creates security log entries on the client computer. If ports 139 or 445 cannot be opened on your network, set the interval to 0 to prevent checking. See Configuring FSSO ports on page 568.

	Dead entry timeout interval	Enter the interval in minutes after which Fortinet Single Sign On Agent purges information for user logons that it cannot verify. The default is 480 minutes (8 hours). Dead entries usually occur because the computer is unreachable (such as in standby mode or disconnected) but the user has not logged off. A common reason for this is when users forget to logoff before leaving the office for the day. You can also prevent dead entry checking by setting the interval to 0.
	IP address change verify interval	Fortinet Single Sign On Agent periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change. IP address verification prevents users from being locked out if they change IP addresses, as may happen with DHCP assigned addresses. Enter the verification interval in seconds. The default is 60 seconds. You can enter 0 to prevent IP address checking if you use static IP addresses. This does not apply to users authenticated through NTLM.
Cache user group lookup result		Enable caching. Caching can reduce group lookups and increase performance.
	Cache expire in (minutes)	Fortinet Single Sign On Agent caches group information for logged-in users. Enter the duration in minutes after which the cache entry expires. If you enter 0, the cache never expires. A long cache expire interval may result in more stale user group information. This can be an issue when a user's group information is changed.
	Clear Group Cache	Clear group information of logged-in users. This affects all logged-in users, and may force them to re-logon.

3. You can select **Save&Close** now or leave the agent configuration window open to complete additional configuration in the following sections.

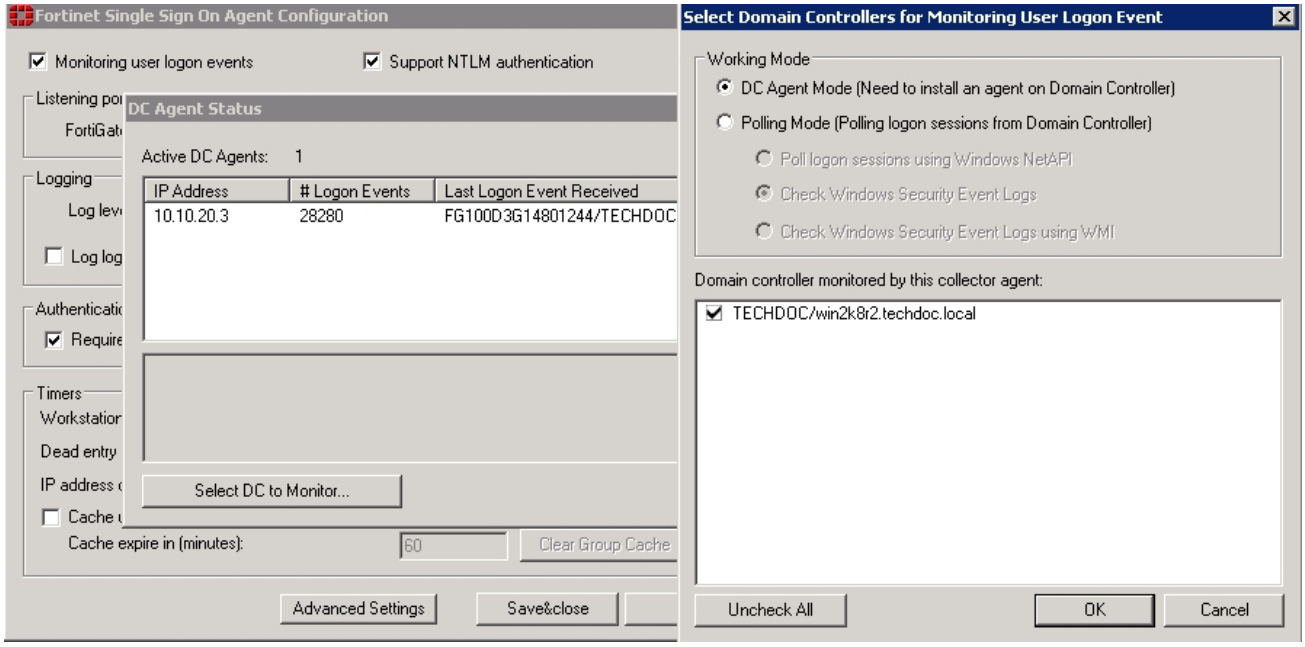
To view the version and build number information for your FSSO Collector Agent configuration, selecting the Fortinet icon in the upper left corner of the Collector agent Configuration screen and select **About Fortinet Single Sign On Agent configuration.**

Selecting Domain Controllers and working mode for monitoring

You can change which DC agents are monitored or change the working mode for logon event monitoring between DC agent mode and polling mode.

When polling mode is selected, it will poll port 445 of the domain controller every few seconds to see who is logged on.

1. From the Start menu select **Programs > Fortinet Fortinet Single Sign-On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Monitored DCs**.
3. Select **Select DC to Monitor**.



4. Choose the **Working Mode:**
   - **DC Agent mode** — a Domain Controller agent monitors user logon events and passes the information to the Collector agent. This provides reliable user logon information, however you must install a DC agent on every domain controller in the domain.
   - **Polling mode** — the Collector agent polls each domain controller for user logon information. Under heavy system load this might provide information less reliably. However installing a DC agent on each domain controller is not required in this mode.
5. You also need to choose the method used to retrieve logon information:
   - Poll logon sessions using Windows NetAPI
   - Check Windows Security Event Logs
   - Check Windows Security Event Logs using WMI

   For more information about these options, see Polling mode on page 548.
6. Select **OK**.
7. Select **Close**.
8. Select **Save & Close**.

Configuring Directory Access settings

The FSSO Collector Agent can access Windows Active Directory in one of two modes:

- Standard — the FSSO Collector Agent receives group information from the Collector agent in the **domain\user** format. This option is available on FortiOS 3.0 and later.
- Advanced — the FSSO Collector Agent obtains user group information using LDAP. The benefit of this method is that it is possible to nest groups within groups. This is option is available on FortiOS 3.0 MR6 and later. The group information is in standard LDAP format.

If you change AD access mode, you must reconfigure your group filters to ensure that the group information is in the correct format.

To configure Directory Access settings:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Directory Access Information**.
   The **Set Directory Access Information** dialog box opens.
3. From the **AD access mode** list, select either **Standard** or **Advanced**.
4. If you selected Advanced AD access mode, select **Advanced Setting** and configure the following settings and then select **OK**:

AD server address	Enter the address of your network's global catalog server.
AD server port	The default AD server port is 3268. This must match your server port.
BaseDN	Enter the Base distinguished name for the global catalog. This is the point in the tree that will be considered the starting point by default-See following example.
Username	If the global catalog accepts your Fortinet Single Sign On Agent agent's credentials, you can leave these fields blank. Otherwise, enter credentials for an account that can access the global catalog.
Password	

BaseDN example

An example DN for Training Fortinet Canada is `ou=training, ou=canada, dc=fortinet, dc=com`. If you set the **BaseDN** to `ou=canada, dc=fortinet, dc=com` then when Fortinet Single Sign On Agent is looking up user credentials, it will only search the Canada organizational unit, instead of all the possible countries in the company. Its a short cut to entering less information and faster searches.

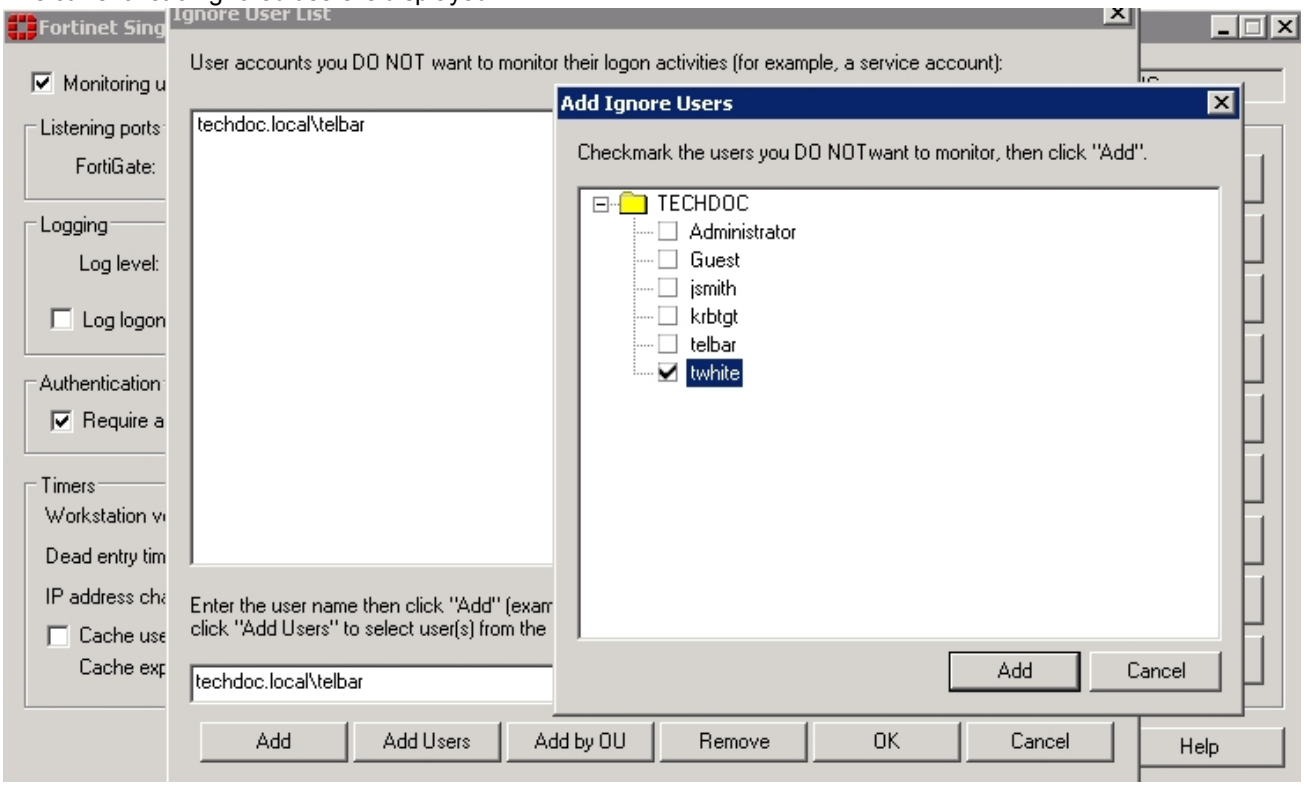
However, you may have problems if you narrow the BaseDN too much when you have international employees from the company visiting different offices. If someone from Fortinet Japan is visiting the Canada office in the example above, their account credentials will not be matched because they are in `ou=japan, dc=fortinet, dc=com` instead of the BaseDN `ou=canada, dc=fortinet, dc=com`. The easy solution is to change the BaseDN to simply be `dc=fortinet, dc=com`. Then any search will check all the users in the company.

Configuring the Ignore User List

The Ignore User List excludes users that do not authenticate to any FortiGate unit, such as system accounts. The logons of these users are not reported to FortiGate units. This reduces the amount of required resources on the FortiGate unit especially when logging logon events to memory.

To configure the Ignore User List:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Ignore User List**.
   The current list of ignored users is displayed:



3. Do any of the following:
   - To remove a user from the list, select the the username and then select **Remove**. The user's login is no longer ignored.
   - To add users to be ignored,
     - enter the username in the format **domain\username** and select **Add** or
     - select **Add Users**, an **Add Ignore Users** window is displayed, checkmark the users you do not want to monitor, then select **Add** or
     - select **Add by OU**, an **Add Ignore Users by OU** window is displayed, select an OU from the directory tree, then select **Add**. All users under the selected OU will be added to the ignore user list.
4. Select **OK**.

Configuring FortiGate group filters

FortiGate group filters actively control which user logon information is sent to each FortiGate unit. You need to configure the group filter list so that each FortiGate unit receives the correct user logon information for the user groups that are named in its security policies. These group filters help limit the traffic sent to the FortiGate unit, and help limit the logon events logged.

The maximum number of Windows AD user groups allowed on a FortiGate depends on the model. Low end models support 256 Windows AD user groups, where mid and high end models support 1024 groups. This is per VDOM if VDOMs are enabled on the FortiGate unit.

You do not need to configure a group filter on the Collector agent if the FortiGate unit retrieves group information from Windows AD using LDAP. In that case, the Collector agent uses the list of groups you selected on the FortiGate unit as its group filter.

The filter list is initially empty. You need to configure filters for your FortiGate units using the Add function. At a minimum, create a default filter that applies to all FortiGate units without a defined filter.

If no filter is defined for a FortiGate unit and there is no default filter, the Collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing the amount of memory the unit uses to store the group list and resulting logs.

To configure a FortiGate group filter:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Group Filters**.
   The FortiGate Filter List opens. It has the following columns:

FortiGate SN	The serial number of the FortiGate unit to which this filter applies.
Description	An optional description of the role of this FortiGate unit.
Monitored Groups	The Windows AD user groups that are relevant to the security policies on this FortiGate unit.
Add	Create a new filter.
Edit	Modify the filter selected in the list.
Remove	Remove the filter selected in the list.
OK	Save the filter list and exit.
Cancel	Cancel changes and exit.

3. Select **Add** to create a new filter. If you want to modify an existing filter, select it in the list and then select **Edit**.
4. Enter the following information and then select **OK**.

Default filter	Select to create the default filter. The default filter applies to any FortiGate unit that does not have a specific filter defined in the list.
FortiGate Serial Number	Enter the serial number of the FortiGate unit to which this filter applies. This field is not available if Default is selected.
Description	Enter a description of this FortiGate unit's role in your network. For example, you could list the resources accessed through this unit. This field is not available if Default is selected.
Monitor the following groups	The Collector agent sends to the FortiGate unit the user logon information for the Windows AD user groups in this list. Edit this list using the Add, Advanced and Remove buttons.
Add	In the preceding single-line field, enter the Windows AD domain name and user group name, and then select Add. If you don't know the exact name, use the Advanced button instead. The format of the entry depends on the AD access mode (see Configuring Directory Access settings on page 565): Standard: Domain\Group Advanced: cn=group, ou=corp, dc=domain
Advanced	Select **Advanced**, select the user groups from the list, and then select **Add**.
Remove	Remove the user groups selected in the monitor list.

Configuring FSSO ports

For FSSO to function properly a small number of TCP and UDP ports must be open through all firewalls on the network. There ports listed in this section assume the default FSSO ports are used.

TCP ports for FSSO agent with client computers

Windows AD records when users log on but not when they log off. For best performance, Fortinet Single Sign On Agent monitors when users log off. To do this, Fortinet Single Sign On Agent needs read-only access to each client computer's registry over TCP port 139 or 445. Open at least one of these ports — ensure it is not blocked by firewalls.

If it is not feasible or acceptable to open TCP port 139 or 445, you can turn off Fortinet Single Sign On Agent logoff detection. To do this, set the Collector agent **workstation verify interval** to 0. The FSSO Collector Agent assumes that the logged on computer remains logged on for the duration of the Collector agent dead entry timeout interval — by default this is eight hours.

Configuring ports on the Collector agent computer

On the computer where you install the Collector agent, you must make sure that the firewall does not block the listening ports for the FortiGate unit and the DC Agent. By default, these are TCP port 8000 and UDP port 8002.

For more information about setting these ports, see Configuring FSSO Advanced Settings on page 574.

Configuring alternate user IP address tracking

In environments where user IP addresses change frequently, you can configure Fortinet Single Sign On Agent to use an alternate method to track user IP address changes. Using this method, Fortinet Single Sign On Agent responds more quickly to user IP address changes because it directly queries workstation IP addresses to match users and IP addresses.

This feature requires FSAE version 3.5.27 or later, Fortinet Single Sign On Agent any version, and FortiOS 3.0 MR7 or later.

To configure alternate user IP address tracking:

1. On the computer where the Collector agent is installed, go to **Start > Run**.
2. Enter `regedit` or `regedt32` and select **OK**.
   The Registry Editor opens.
3. Find the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent.
4. Set the supportFSAEauth value (dword) to 00000001.
   If needed, create this new dword.
5. Close the Registry Editor.
6. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
7. Select **Apply**.
   The Fortinet Single Sign On Agent service restarts with the updated registry settings.

Viewing FSSO component status

It is important to know the status of both your Collector agents and DC agents.

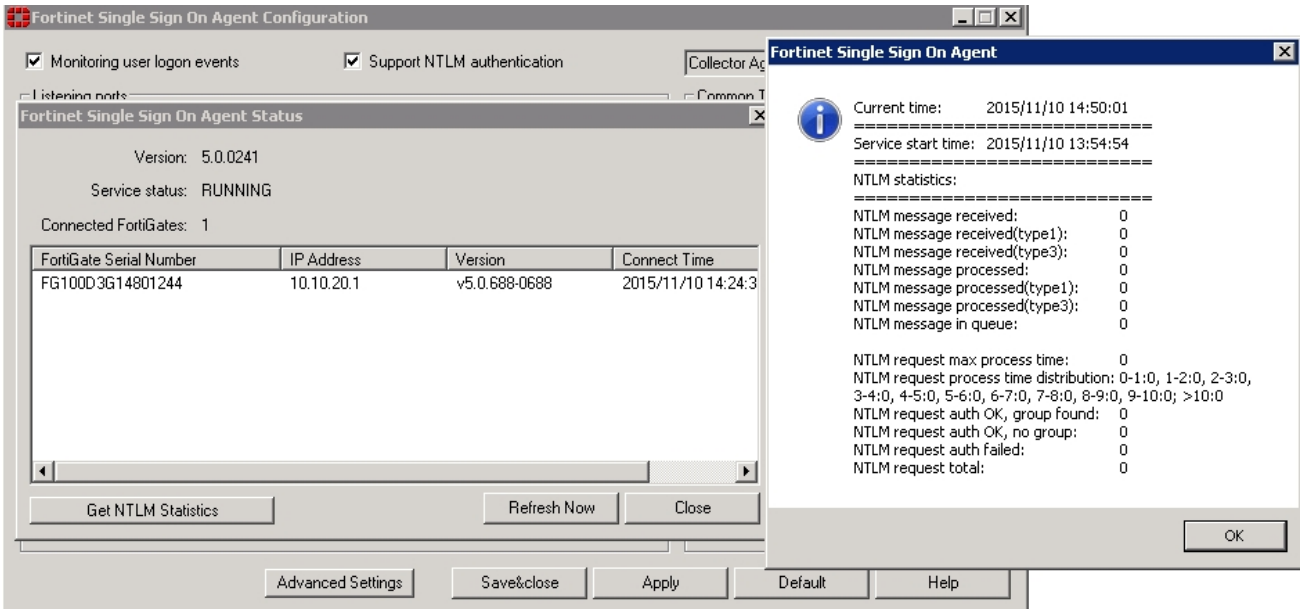
Viewing Collector agent status

Use the **Show Service Status** to view your Collector agent information in the Status window. The Status window displays:

- the version of the software
- the status of the service
- the number of connected FortiGate units
- connected FortiGate information such as serial number, IP address, and connect time

To view Collector agent status:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Service Status**.
   The Fortinet Single Sign On Collector agent Status window opens.
3. Optionally select **Get NTLM statistics** in the Status window to display NTLM information such as number of messages received, processed, failed, in the queue.



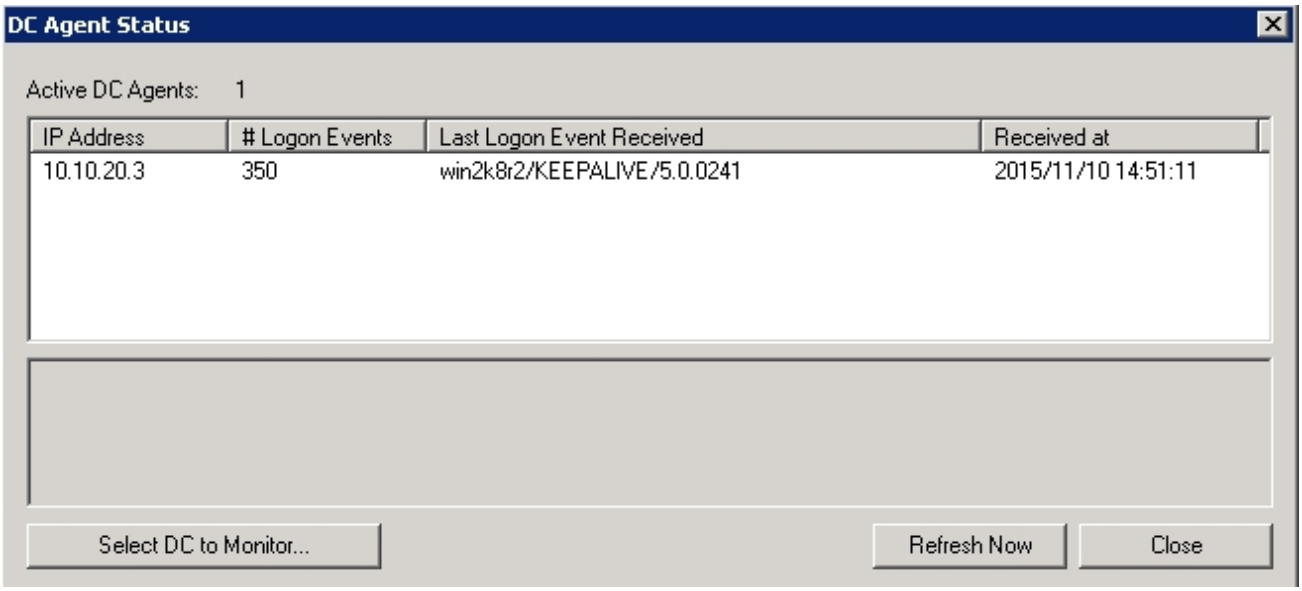
Viewing DC agent status

Use the **Show Monitored DCs** to view the status of DC agents.

To view domain controller agent status:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Monitored DCs**.
   For each DC Agent, the following information is displayed:
   - IP address
   - number of logon events received
   - the last logon event
   - when last logon was received

To change which DC agents are monitored or change the working mode for logon event monitoring, select **Select DC to Monitor**



Configuring the FSSO TS agent for Citrix

The FSSO TS agent works with the same FSSO Collector agent that is used for integration with Windows Active Directory. Install the Collector agent first. Follow the Collector agent installation procedure in Collector agent installation on page 554.

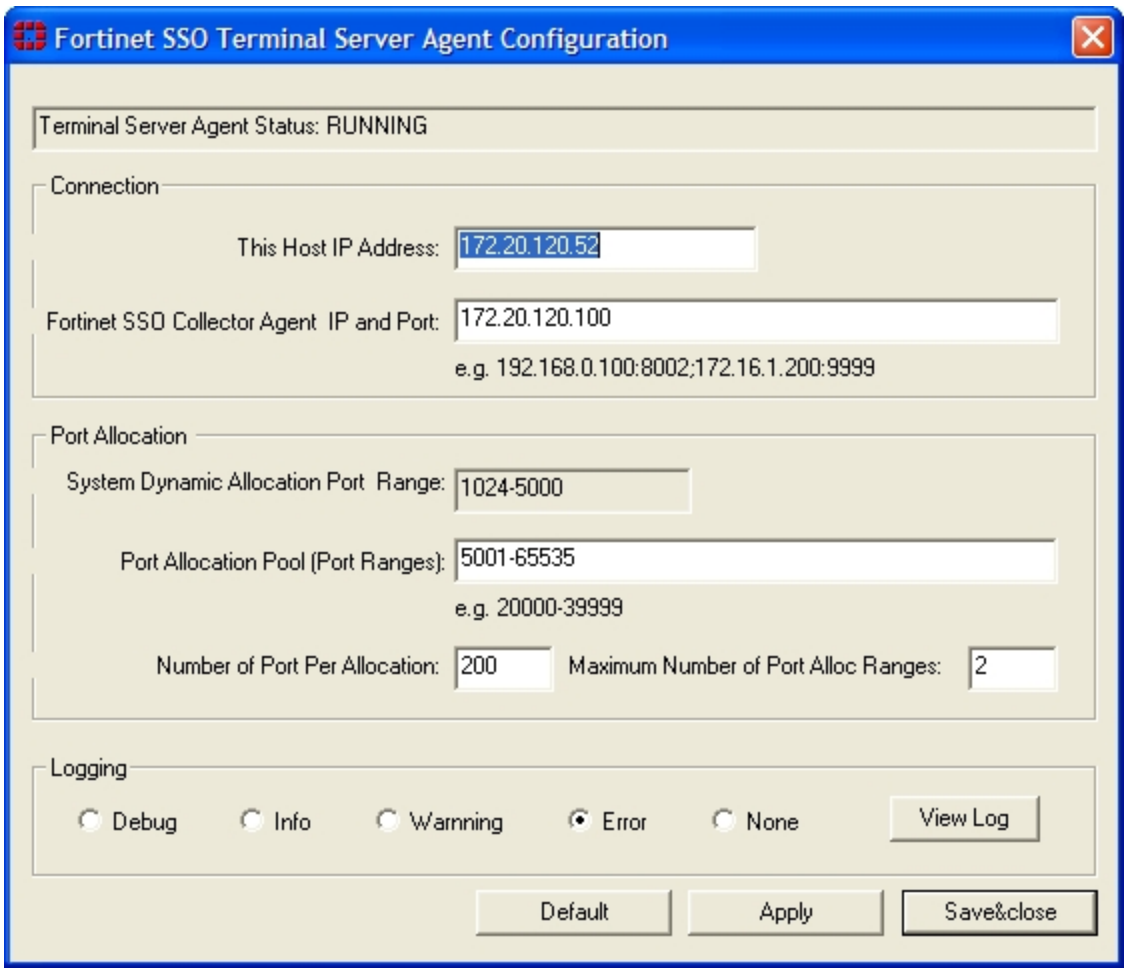
Configuration steps include:

- Install the Fortinet Citrix FSSO agent on the Citrix server.
- Install the Fortinet FSSO collector on a server on the network.
- Add the Citrix FSSO agent to the FortiGate Single-sign-On configuration.
- Add Citrix FSSO groups and users to an FSSO user group.
- Add an FSSO identity-based security policy that includes the Citrix FSSO user groups.

To change the TS agent configuration, select from the Start menu **Programs > Fortinet > Fortinet Single Sign-On Agent > TSAgent Config**. In addition to the host and Collector agent IP addresses that you set during installation, you can adjust port allocations for Citrix users. When a Citrix user logs on, the TS agent assigns that user a range of ports. By default each user has a range of 200 ports.

Fortinet SSO Collector Agent IP and Port needs to point to the current configured listening port on the collector which is port 8002 by default. Though it may be configured to a custom port.

Configuring the TS agent



Configuring FSSO with Novell networks

You need to configure the eDirectory agent for it to communicate with eDirectory servers. You may have provided some of this information during installation.

This section includes:

- Configuring the eDirectory agent
- Adding an eDirectory server
- Configuring a group filter

Configuring the eDirectory agent

You need to configure the eDirectory agent for it to communicate with eDirectory servers.

To configure the eDirectory agent:

1. From the Start menu select **Programs > Fortinet > eDirectory Agent > eDirectory Config Utility**.
2. The eDirectory Agent Configuration Utility dialog opens. Enter the following information and select **OK**.

eDirectory Authentication	
Username	Enter a username that has access to the eDirectory, using LDAP format.
Password	Enter the password.
Listening port	Enter the TCP port on which Fortinet Single Sign On Agent listens for connections from FortiGate units. The default is 8000. You can change the port if necessary.
Refresh interval	Enter the interval in seconds between polls of the eDirectory server to check for new logons. The default is 30 seconds.

FortiGate Connection Authentication	
Require authenticated connection from FortiGate	Select to require the FortiGate unit to authenticate before connecting to the eDirectory Agent.
Password	Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “FortinetCanada”.
User logon Info Search Method	Select how the eDirectory agent accesses user logon information: **LDAP** or **Native** (Novell API). LDAP is the default. If you select **Native**, you must also have the Novell Client installed on the PC.

Logging	
Log file size limit (MB)	Enter the maximum size for the log file in MB.
View Log	View the current log file.
Dump Session	List the currently logged-on users in the log file. This can be useful for troubleshooting.
Log level	Select **Debug, Info**, **Warning** or **Error** as the minimum severity level of message to log or select **None** to disable logging.

eDirectory Server List	
Add	Add an eDirectory server. See Adding an eDirectory server on page 574.
Delete	Delete the selected eDirectory server.
Edit	Modify the settings for the selected server.
Set Group Filters...	Select the user groups whose user logons will be reported to the FortiGate unit. This is used only if user groups are not selected on the FortiGate unit.

Adding an eDirectory server

Once the eDirectory agent is configured, you add one or more eDirectory servers.

To add an eDirectory server:

1. In the eDirectory Agent Configuration Utility dialog box (see the preceding procedure, Configuring the eDirectory agent), select **Add**.
2. The eDirectory Setup dialog box opens. Enter the following information and select OK:

eDirectory Server Address	Enter the IP address of the eDirectory server.
Port	If the eDirectory server does not use the default port 389, clear the **Default** check box and enter the port number.
Use default credential	Select to use the credentials specified in the eDirectory Configuration Utility. See Configuring the eDirectory agent on page 572. Otherwise, leave the check box clear and enter a username and Password below.
User name	Enter a username that has access to the eDirectory, using LDAP format.
User password	Enter the password.
Use secure connection (SSL)	Select to connect to the eDirectory server using SSL security.
Search Base DN	Enter the base Distinguished Name for the user search.

Configuring a group filter

The eDirectory agent sends user logon information to the FortiGate unit for all user groups unless you either configure an LDAP server entry for the eDirectory on the FortiGate unit and select the groups that you want to monitor or configure the group filter on the eDirectory agent.

If both the FortiGate LDAP configuration and the eDirectory agent group filter are present, the FortiGate user group selections are used.

To configure the group filter:

1. From the Start menu select **Programs > Fortinet > eDirectory Agent > eDirectory Config Utility**.
2. Select **Set Group Filters**.
3. Do one of the following:
   - Enter group names, then select **Add**.
   - Select **Advanced**, select groups, and then select **Add**.
4. Select **OK**.

Configuring FSSO Advanced Settings

Depending on your network topologies and requirement, you may need to configure advanced settings in the FSSO Colloctor agent.To do so, from the Start menu, select **Programs > Fortinet > Fortinet Single Sign-On Agent > Configure Fortinet Single Sign-On Agent**, then from the **Common Tasks** section, select **Advanced Settings**.

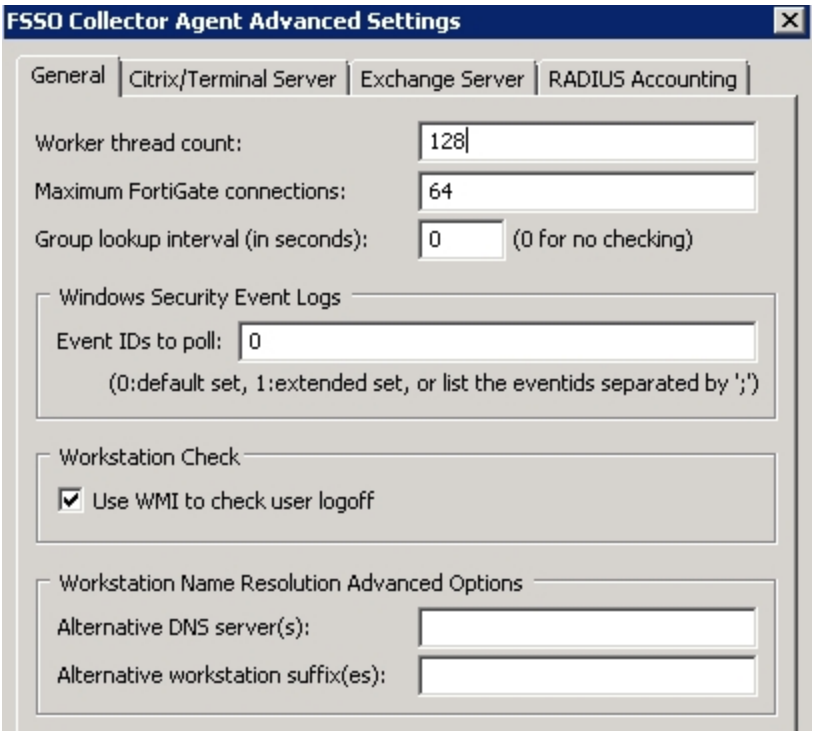
This section include :

- General Settings
- Citrix/Terminal Server
- Exchange Server
- RADIUS Accounting

General Settings

In the General tab, enter the following information and select **OK**.

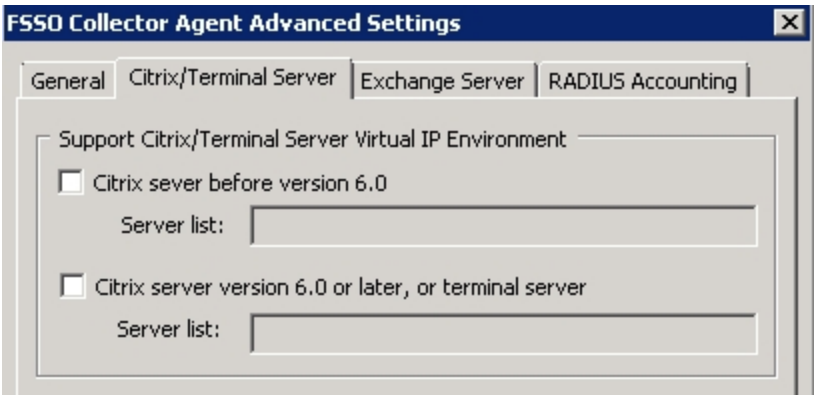
Worker thread count	Number of threads started in the CA process. Default is128 on CA version 5.0.0241.
Maximum FortiGate connections	Number of FortiGates can be connected to the CA. Default is 64.
Group look-up interval	The interval in seconds to lookup users/groups. If an AD group membership of currently logged on user, CA can detect this and update information on the FortiGate. Enter 0 for no checking.
Windows security Event logs	Choose the event logs to poll.
Event IDs to poll	0:Default set, it includes Kerberos authentication event logs : 672 for Windows server 2003, 4768 for Windows server 2008 and 2012 and NTLM authentication event logs : 680 for Windows server 2003, 4776 for Windows server 2008 and 2012. 1: Extended set, it includes Kerberos service ticket event logs : 673 for Windows server 2003, 4769 for Windows server 2008 and 2012. Service tickets are obtained whenever a user or computer accesses a server on the network. List the event ids separated by ";".
Workstation Check	Optianally enable **Use WMI to check user logoff** for the collector agent to query whether users is still logged on.
Workstation Name Resolution Advance Options	
Alternative DNS server (s)	Collector Agent uses the DNS server configured on the machine it is running on by default. If CA should use another DNS server then one or more alternative DNS server can be configured here.
Alternative workstation suffix(es)	If only host name is available CA uses the default domain suffix to build a FQDN for DNS queries. In case CA should use a different suffix, it can be configured as well.



Citrix/Terminal Server

In the Citrix/Terminal Server tab, enter the following information and select **OK**.

Support Citrix/Terminal Server Virtual IP Environment	When Citrix server are configured with VIP, CA can get user logon events from theses server. Citrix changed their interface and data format so version of Citrix server is important.
Citrix server before version 6.0	Enable this option if you Citrix server version is before 6.0.
Server list	Enter the list of servers separated by colon.
Citrix server version 6.0 or later, or Terminal Server	Enable this option if you Citrix server version is 6.0 or later.
Server list	Enter the list of servers separated by colon.

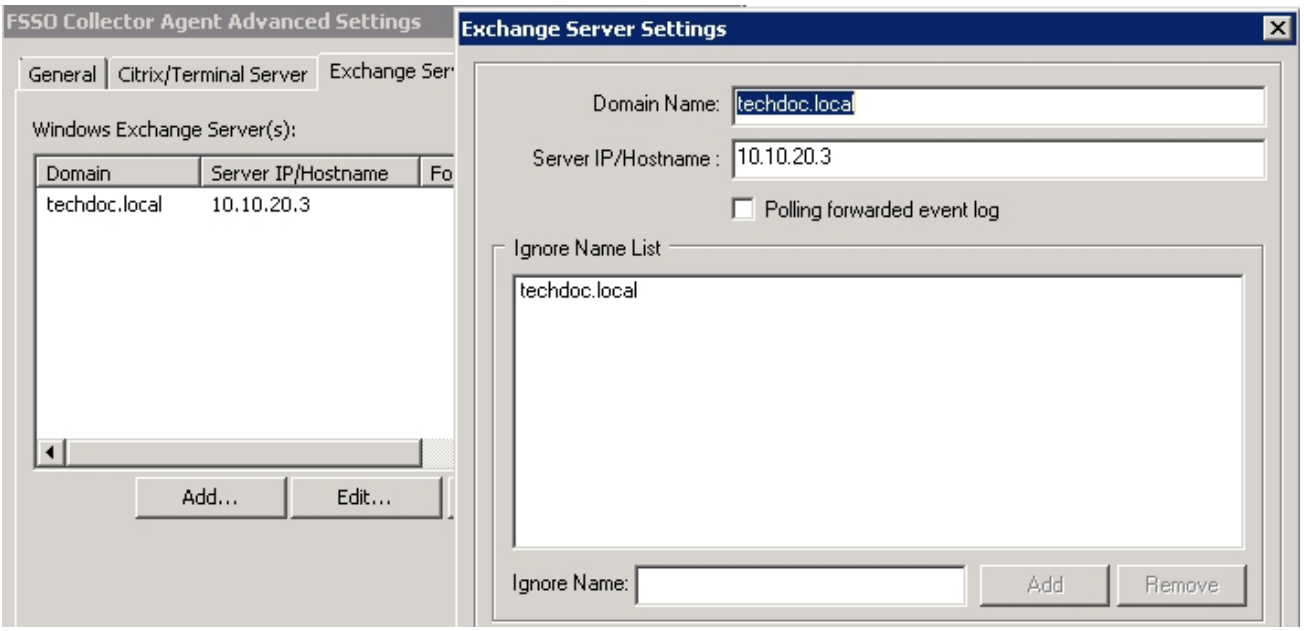


Exchange Server

FSSO supports monitoring Microsoft Exchange Server. This is useful for situation that the user use the domain account to access their email, but client device might or might not be in the domain. Support for Exchange server is configured on the Back-end FSSO collector agent under **Advanced Settings** > **Exchange Server**.

Select **Add** and enter the following information and select **OK**.

Domain Name	Enter your domain name.
Server IP/Hostname	Enter the IP address or the hostname of your exchange server.
Polling forwarded event log	This option for scenarios when you do not want that CA polls the Exchange Server logs directly. In this case you need to configure event log forwarding on the Exchange server. Exchange event logs can be forwarded to any member server. If you enable this, instead of the IP of the Exchange server configured in the previous step, you must then configure the IP of this member server. CA will then contact the member server.
Ignore Name	Because CA will also check Windows log files for logon events and when a user authenticates to Exchange Server there is also a logon event in Windows event log, which CA will read and this will overwrite the Exchange Server logon event (ES-EventLog) on CA. So it is recommended to set the ignore list to the domain the user belongs to. To do so, enter the domain name in the **Ignore Name** field and select **Add**.



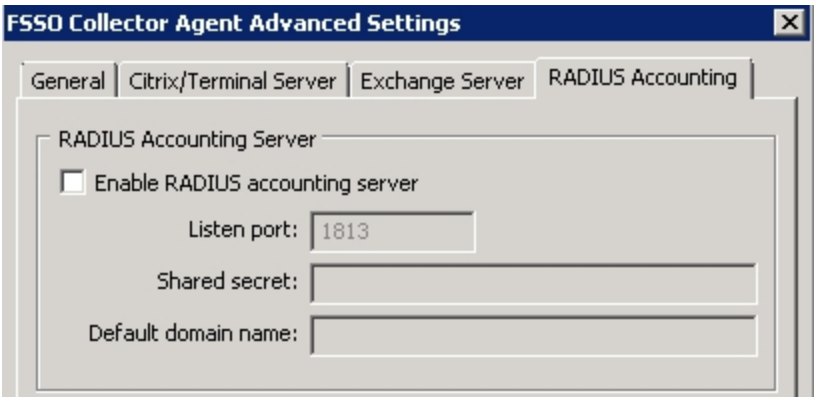
RADIUS Accounting

A RADIUS server must be configured in your network to send accounting messages to the Collector Agent which can be configured to work with most RADIUS-based accounting systems. In most cases, you only need to do the following to your RADIUS accounting system:

- Add a user group name field to customer accounts on the RADIUS server so that the name is added to the RADIUS Start record sent by the accounting system to the Collector Agent. User group names do not need to be added for all users, only to the accounts of users who will use RADIUS Accounting feature on the Collector Agent.
- Configure your accounting system to send RADIUS Start records to the Collector Agent.

The Collocter Agent should be configured to listen for RADIUS accounting messages as following.

RADIUS Accounting Server	
Enable RADIUS Accounting Server	Enable this option to allow the CA to gather information about authenticated users via a RADIUS server and send these information to the FortiGate unit for monitoring.
Listen port	The port on which CA listens for RADIUS accounting messages. Default RADIUS accounting is 1813, but if RADIUS server sends accounting messages on different port, value can be configured here.
Shared secret	Common secret between CA and RADIUS server.
Default domain name	This should be the AD domain for which this CA is configured. In this case user name in RADIUS accounting message can be in simple format like `user1`. If this value is empty, then user name in RADIUS accounting message must be in one of these formats `user1@domain`, `Domain\user1` or `domain/user1`. CA will use user name and domain to query group membership of user. Client IP address (Framed IP) should also be in RADIUS accounting message, so that CA can forward user name, IP address and groups to the FortiGate.



Configuring FSSO on FortiGate units

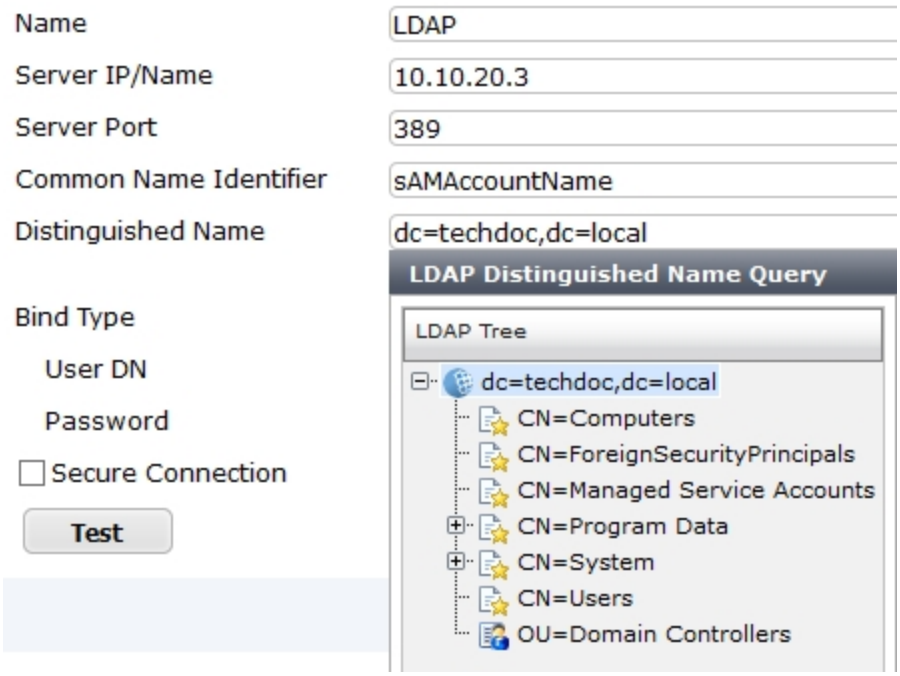
To configure your FortiGate unit to operate with agent-based FSSO, you

- Configure any access to LDAP servers that might be necessary. Skip this step if you are using FSSO Standard mode. See Configuring LDAP server access on page 579.
- Specify the Collector agent or Novell eDirectory agent that will provide user logon information. See Specifying your Collector agents or Novell eDirectory agents on page 581.
- Add Active Directory user groups to FortiGate user groups. See Creating Fortinet Single Sign-On (FSSO) user groups on page 582.
- Create security policies for FSSO-authenticated groups. See Creating security policies on page 583.
- Optionally, specify a guest security policy to allow guest access. See Enabling guest access through FSSO security policies on page 584.

Configuring LDAP server access

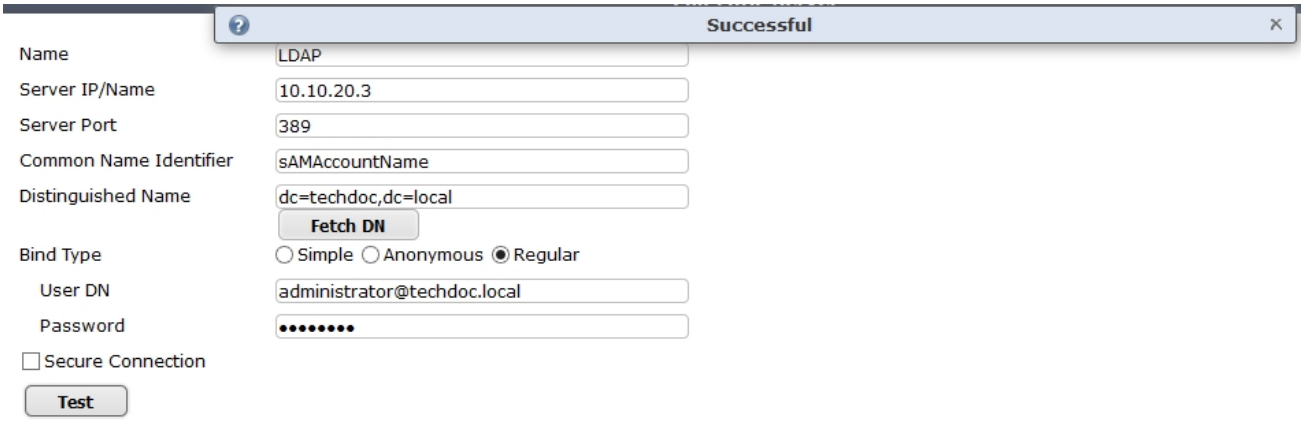
LDAP access is required if your network has a Novell eDirectory agent or a Collector agent using Windows Advanced AD access mode. If you are using FSSO Standard mode, go to Specifying your Collector agents or Novell eDirectory agents on page 581.

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the **Server IP/Name** and **Server Port** (default 389).
3. In the **Common Name Identifier** field, enter **sAMAccountName**.The default common name identifier is `cn`. This is correct for most LDAP servers. However some servers use other identifiers such as `uid`.
4. In the **Distinguished Name** field, enter your organization distinguished name. In this example, Distinguished Name is dc=techdoc,dc=local
5. Select **Fetch DN**, this will fetch the Windows AD directory.



6. Set **Bind Type** to **Regular.**
7. In the **User DN** field, enter the administrative account name that you created for FSSO.
   For example, if the account is administrator, enter “administrator@techdoc.local”.
8. Enter the administrative account password in the **Password** field.
9. Optionally select **Secure Connection**.
   - In the **Protocol** field, select **LDAPS** or **STARTTLS**.
   - In the **Certificate** field, select the appropriate certificate for authentication.

   Note that you need to configure the Windows AD for secure connection accordingly.
10. Select **OK**.
11. Test your configuration by selecting the **Test** button. A successful message confirming the right settings appears.



To configure LDAP for FSSO - CLI example:

```
config user ldap
   edit LDAP
      set server 10.10.20.3
```

```
        set cnid sAMAccountName
        set dn dc=techdoc,dc=local
        set type regular
        set username administrator@techdoc.local
        set password <your_password>
    next
end
```

Specifying your Collector agents or Novell eDirectory agents

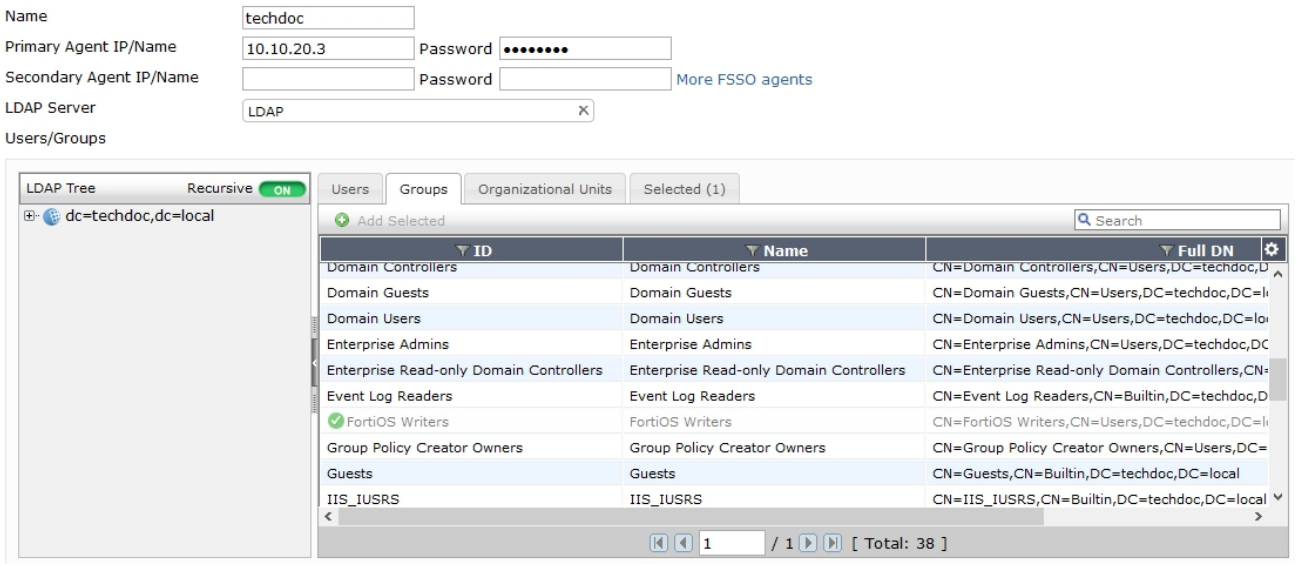
You need to configure the FortiGate unit to access at least one Collector agent or Novell eDirectory agent. You can specify up to five servers on which you have installed a Collector or eDirectory agent. The FortiGate unit accesses these servers in the order that they appear in the list. If a server becomes unavailable, the next one in the list is tried.

To specify Collector agents - web-based manager:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **Fortinet Single-Sign-On Agent**.
3. Enter a **Name** for the Windows AD server. This name appears in the list of Windows AD servers when you create user groups.
4. Enter the following information for each of up to five collector agents and select **OK**:

Agent IP/Name	Enter the IP address or the name of the server where this agent is installed. Maximum name length is 63 characters. If the TCP port used for FSSO is not the default, 8000, you can change the setting in the CLI using the `config user fsso` command. See Configuring Collector agent settings on page 561.
Password	Enter the password for the Collector agent or eDirectory agent. For the Collector agent, this is required only if you configured the agent to require authenticated access.

5. For Novell eDirectory or Windows AD with Collector agent in Advanced AD access mode select the **LDAP Server** you configured previously. See Configuring LDAP server access on page 579.
6. In **Users/Groups**, select the **Users** or **Groups** or **Organizational Units** tab and then select the users or groups or OU that you want to monitor.
7. Select **OK**.



To specify the FSSO Collector agent - CLI:

In this example, the SSO server name is techdoc and the LDAP server is LDAP.

```
config user fsso
   edit techdoc
      set ldap-server LDAP
      set password <your_password>
      set server 10.10.20.3
      set port 8000
   end
```

Creating Fortinet Single Sign-On (FSSO) user groups

You cannot use Windows or Novell groups directly in FortiGate security policies. You must create FortiGate user groups of the FSSO type and add Windows or Novell groups to them.

To create a user group for FSSO authentication - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select **Create New**.
   The New User Group dialog box opens.
3. In the **Name** box, enter a name for the group, FSSO_Internet_users for example.
4. In **Type**, select **Fortinet Single Sign-On (FSSO)**.
5. In **Members**, select the required **FSSO** groups.
6. Select **OK**.

To create the FSSO_Internet-users user group - CLI :

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
```

```
end
```

Creating security policies

Policies that require FSSO authentication are very similar to other security policies. Using identity-based policies, you can configure access that depends on the FSSO user group. This allows each FSSO user group to have its own level of access to its own group of services

In this situation, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate

For the following procedure, the internal interface is `port1` and the external interface connected to the Internet is `port2`. There is an address group for the internal network called `company_network`. The FSSO user group is called `fsso_group`, and the FSSO RADIUS server is `fsso_rad_server`.

To configure an FSSO authentication security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IP4** and select **Create New**.
2. Enter the following information.

Incoming Interface	port1
Source Address	company_network
Source User(s)	`fsso_group`
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	HTTP, HTTPS, FTP, and Telnet
Action	ACCEPT
NAT	ON
UTM Security Profiles	ON for AntiVirus, IPS, Web Filter, and Email Filter, all using default profiles.
Log Allowed Traffic	ON. Select **Security Events**.

3. Select **OK**.
4. Ensure the FSSO authentication policy is higher in the policy list than more general policies for the same interfaces.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port1
```

```
    set dstintf port2
    set srcaddr company_network
    set dstaddr all
    set action accept
    set groups fsso_group
    set schedule always
    set service HTTP HTTPS FTP TELNET
    set nat enable
end
```

Here is an example of how this FSSO authentication policy is used. Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy intercepts the session, checks with the FSSO Collector agent to verify the user's identity and credentials, and then if everything is verified the user is allowed access to the Internet.

Users belonging to multiple groups

Before FSSO 4.0 MR3, if a user belonged to multiple user groups, the first security policy to match any group that user belonged too was the only security policy applied. If that specific group did not have access to this protocol or resource where another group did, the user was still denied access. For example, `test_user` belongs to `group1` and `group2`. There are two FSSO authentication policies — one matches `group1` to authenticate FTP traffic and one matches `group2` to authenticate email traffic. The `group1` policy is at the top of the list of policies. If `test_user` wants to access an email server, the first policy encountered for a group `test_user` belongs to is the `group1` policy which does not allow email access and `test_user` is denied access. This is despite the next policy allowing access to email. If the order was reversed in this case, the traffic would be matched and the user's traffic would be allowed through the firewall. However if the policy order was reversed, FTP traffic would not be matched.

As of FSSO 4.0 MR3, if a user belongs to multiple groups multiple then attempts to match the group are attempted if applicable. Using the above example, when the attempt to match the `group1` policy is made and fails, the next policy with a group that `test_user` is a member of is attempted. In this case, the next policy is matched and access is granted to the email server.

When configuring this example the only difference between the policies is the services that are listed and the FSSO user group name.

Authenticating through multiple groups allows administrators to assign groups for specific services, and users who are members of each group have access to those services. For example there could be an FTP group, an email group, and a Telnet group.

Enabling guest access through FSSO security policies

You can enable guest users to access FSSO security policies. Guests are users who are unknown to the Windows AD or Novell network and servers that do not logon to a Windows AD domain.

To enable guest access in your FSSO security policy, add an identity-based policy assigned to the built-in user group `SSO_Guest_Users`. Specify the services, schedule and protection profile that apply to guest users — typically guests receive reduced access to a reduced set of services. Creating security policies on page 583

FortiOS FSSO log messages

There are two types of FortiOS log messages — firewall and event. FSSO-related log messages are generated from authentication events. These include user logon and log off events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues. For more information on firewall logging, see "Enabling security logging". For more information on logging, see the FortiOS Handbook Log and Reporting guide.

Enabling authentication event logging

For the FortiGate unit to log events, that specific type of event must be enabled under logging.

When VDOMs are enabled certain options may not be available, such as CPU and memory usage events. You can enable event logs only when you are logged on to a VDOM; you cannot enable event logs globally.

To ensure you log all the events need, set the minimum log level to Notification or Information. Firewall logging requires Notification as a minimum. The closer to Debug level, the more information will be logged. While this extra information is useful, you must

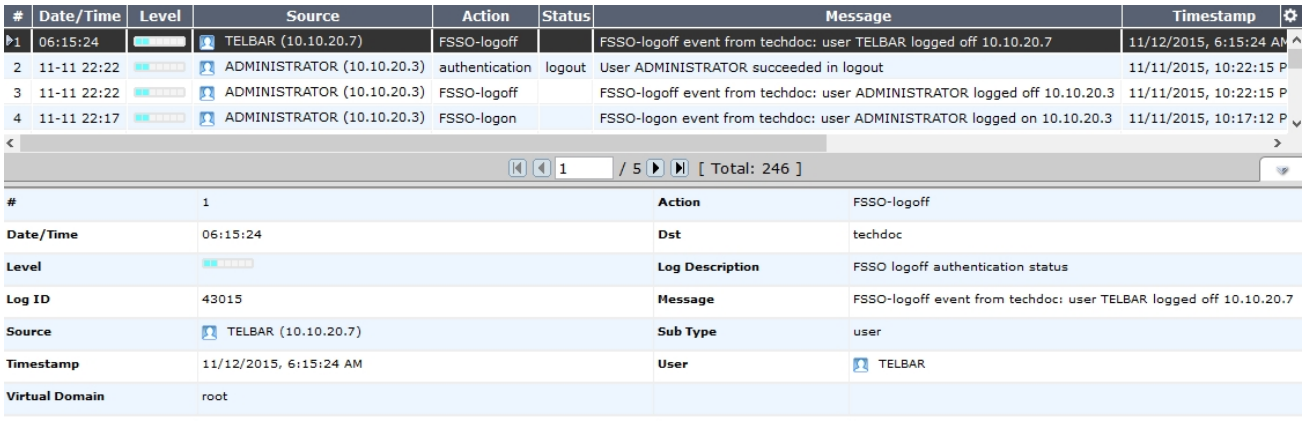
To enable event logging:

1. Go to **Log&Report > Log Config > Log Settings**.
2. In **Event Logging**, select:

System activity event	All system-related events, such as ping server failure and gateway status.
User activity event	All administration events, such as user logins, resets, and configuration updates.

3. Optionally you can enable any or all of the other logging event options.
4. Select **Apply**.

Authentication log messages



List of FSSO related log messages

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication was successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication was successful
43017	Notification	NTLM authentication failed

For more information on logging, see the FortiOS Handbook Log and Reporting guide.

Testing FSSO

Once FSSO is configured, you can easily test to ensure your configuration is working as expected. For additional FSSO testing, see Troubleshooting FSSO on page 587.

1. Logon to one of the stations on the FSSO domain, and access an Internet resource.
2. Connect to the CLI of the FortiGate unit, and if possible log the output.
3. Enter the following command:
   ```
   diagnose debug authd fsso list
   ```
4. Check the output. If FSSO is functioning properly you will see something similar to the following:
   ```
   ----FSSO logons----
   IP: 10.10.20.3 User: ADMINISTRATOR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL
       Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf: FortiOS_Writers
   IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL
       Workstation: TELBAR-PC7.TECHDOC.LOCAL
   Total number of logons listed: 2, filtered: 0
   ----end of FSSO logons----
   ```
   The exact information will vary based on your installation.
5. Check the FortiGate event log, for FSSO-auth action or other FSSO related events with FSSO information in the message field.
6. To check server connectivity, run the following commands from the CLI:
   ```
   FGT# diagnose debug enable
   FGT# diagnose debug authd fsso server-status
   ```

```
FGT# Server Name Connection Status Version
     ----------- ----------------- -------
     techdoc       connected FSSO 5.0.0241
```

Troubleshooting FSSO

When installing, configuring, and working with FSSO some problems are quite common. A selection of these problems follows including explanations and solutions.

Some common Windows AD problems include:

- General troubleshooting tips for FSSO
- Users on a particular computer (IP address) cannot access the network
- Guest users do not have access to network
- Can't find the DCagent service
- User logon events not received by FSSO Collector agent
- Mac OS X users can't access external resources after waking from sleep mode

General troubleshooting tips for FSSO

The following tips are useful in many FSSO troubleshooting situations.

- Ensure all firewalls are allowing the FSSO required ports through.
  FSSO has a number of required ports that must be allowed through all firewalls or connections will fail. These include: ports 139, 389 (LDAP), 445, 636 (LDAP) 8000, and 8002.
- Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit.
  If not the Collector agent does not have this amount of bandwidth, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available.

Users on a particular computer (IP address) cannot access the network

Windows AD Domain Controller agent gets the username and workstation where the logon attempt is coming from. If there are two computers with the same IP address and the same user trying to logon, it is possible for the authentication system to become confused and believe that the user on computer_1 is actually trying to access computer_2.

Windows AD does not track when a user logs out. It is possible that a user logs out on one computer, and immediate logs onto a second computer while the system still believes the user is logged on the original computer. While this is allowed, information that is intended for the session on one computer may mistakenly end up going to the other computer instead. The result would look similar to a hijacked session.

Solutions

- Ensure each computer has separate IP addresses.
- Encourage users to logout on one machine before logging onto another machine.
- If multiple users have the same username, change the usernames to be unique.
- Shorten timeout timer to flush inactive sessions after a shorter time.

Guest users do not have access to network

A group of guest users was created, but they don't have access.

Solution

The group of the guest users was not included in a policy, so they do not fall under the guest account. To give them access, associate their group with a security policy.

Additionally, there is a default group called **SSO_Guest_Users**. Ensure that group is part of an identity-based security policy to allow traffic.

Can't find the DCagent service

The DCagent service can't be found in the list of regular windows services. This is because it has no associated Windows service.

Instead DCagent is really `dcagent.dll` and is located in the `Windows\system32` folder. This DLL file is loaded when windows boots up and it intercepts all logon events processed by the domain controller to send these events to the Collector agent (CA).

Solution

To verify that the DCagent is installed properly

1. Check that DCagent.dll exists in `Windows\system32` folder.
2. Check that the registry key exists: `[HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\dcagent]`

If both exist, the DCagent is properly installed.

User logon events not received by FSSO Collector agent

When a warning dialog is present on the screen on the Collector agent computer, the Collector agent will not receive any logon events. Once the dialog has been closed normal operation will resume.

If polling mode is enabled, it is possible the polling interval is too large. Use a shorter polling interval to ensure the collector agent is capturing all logon events.

If NetAPI polling mode is enabled, consider switching to Event logs or Event Logs using WMI polling as it provides better accuracy.

Mac OS X users can't access external resources after waking from sleep mode

When client computers running Mac OS X (10.6.X and higher) wake up from sleep mode, the user must authenticate again to be able to access external resources. If the user does not re-authenticate, the user will maintain access to internal web sites, but will be unable to access any external resources.

This issue is caused by Mac OS X not providing sufficient information to the FSSO. This results in the FortiGate blocking access to the user because they cannot be authenticated.

Solution

The security settings on client computer(s) must be configured to require that a username and password be entered when exiting sleep mode or screen saver. With this feature enabled in Mac OS X, the FortiGate will receive the authentication information it requires to authenticate the user and allow them access.

Note that if the user reverts their settings to disable the password requirement, this will cause the issue to reappear.

SSO using RADIUS accounting records

A FortiGate unit can authenticate users transparently who have already authenticated on an external RADIUS server. Based on the user group to which the user belongs, the security policy applies the appropriate UTM profiles. RADIUS SSO is relatively simple because the FortiGate unit does not interact with the RADIUS server, it only monitors RADIUS accounting records that the server emits. These records include the user's IP address and user group.

After the initial set-up, changes to the user database, including changes to user group memberships, are made on the external RADIUS server, not on the FortiGate unit.

This section describes:

- User's view of RADIUS SSO authentication
- Configuration Overview
- Configuring the RADIUS server
- Creating the FortiGate RADIUS SSO agent
- Defining local user groups for RADIUS SSO
- Creating security policies
- Example: webfiltering for student and teacher accounts

User's view of RADIUS SSO authentication

For the user, RADIUS SSO authentication is simple:

- The user connects to the RADIUS server and authenticates.
- The user attempts to connect to a network resource that is reached through a FortiGate unit. Authentication is required for access, but the user connects to the destination without being asked for logon credentials because the FortiGate unit knows that the user is already authenticated. FortiOS applies UTM features appropriate to the user groups that the user belongs to.

Configuration Overview

The general steps to implement RADIUS Single Sign-On are:

1. If necessary, configure your RADIUS server. The user database needs to include user group information and the server needs to send accounting messages.
2. Create the FortiGate RADIUS SSO agent.
3. Define local user groups that map to RADIUS groups.
4. Create a security policy which specifies the user groups that are permitted access.

Configuring the RADIUS server

You can configure FortiGate RSSO to work with most RADIUS-based accounting systems. In most cases, you only need to do the following to your RADIUS accounting system:

- Add a user group name field to customer accounts on the RADIUS server so that the name is added to the RADIUS Start record sent by the accounting system to the FortiOS unit. User group names do not need to be added for all

users, only to the accounts of users who will use RSSO feature on the FortiGate unit.

- Configure your accounting system to send RADIUS Start records to the FortiOS unit. You can send the RADIUS Start records to any FortiGate network interface. If your FortiGate unit is operating with virtual domains (VDOMs) enabled, the RADIUS Start records must be sent to a network interface in the management VDOM.

Creating the FortiGate RADIUS SSO agent

Once you define a RADIUS SSO (RSSO) agent, the FortiGate unit will accept user logon information from any RADIUS server that has the same shared secret. You can create only one RSSO agent in each VDOM.

Before you create the RSSO agent, you need to allow RADIUS accounting information on the interface that connects to the RADIUS server.

To enable RADIUS access on the interface - web-based manager:

1. Go to **System > Network > Interfaces** and edit the interface to which the RADIUS server connected.
2. Select **Listen for RADIUS Accounting Messages**.
3. Select **OK**.

To enable RADIUS access on the interface - CLI:

In this example, the port2 interface is used.

```
config system interface
   edit port2
      set allowaccess radius-acct
   end
```

To create a RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On Agent**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.

To create a RADIUS SSO agent - CLI

```
config user radius
   edit RSSO_Agent
      set rsso enable
      set rsso-validate-request-secret enable
      set rsso-secret <your secret>
      set rsso-radius-response enable
   end
```

Selecting which RADIUS attributes are used for RSSO

For RADIUS SSO to work, FortiOS needs to know the user's endpoint identifier (usually IP address) and RADIUS user group. There are default RADIUS attributes where FortiOS expects this information, but you can change these attributes in the `config user radius` CLI command.

RSSO information and RADIUS attribute defaults

RSSO Information	RADIUS Attribute	CLI field
Endpoint identifier	Calling-Station-ID	`rsso-endpoint-attribute`
Endpoint block attribute	Called-Station-ID	`rsso-endpoint-block-attribute`
User group	Class	`sso-attribute`

The Endpoint block attribute can be used to block or allow a user. If the attribute value is set to the name of an attribute that indicates whether to block or allow, FortiOS blocks or allows respectively all traffic from that user's IP address. The RSSO fields are visible only when `rsso` is set to `enable`.

Configuring logging for RSSO

In the `config user radius` CLI command, you can set the following flags in the `rsso-log-flags` field to determine which types of RSSO-related events are logged:

- `protocol-error` — A RADIUS protocol error occurred.
- `profile-missing` — FortiOS cannot find a user group name in a RADIUS start message that matches the name of an RSSO user group in FortiOS.
- `accounting-stop-missed` — a user context entry expired without FortiOS receiving a RADIUS Stop message.
- `accounting-event` — FortiOS did not find the expected information in a RADIUS record.
- `endpoint-block` — FortiOS blocked a user because the RADIUS record's endpoint block attribute had the value "Block".
- `radiusd-other` — Other events, described in the log message.

Defining local user groups for RADIUS SSO

You cannot use RADIUS user groups directly in security policies. Instead, you create locally-defined user groups on the FortiGate unit and associate each of them with a RADIUS user group.

To define local user groups for RADIUS SSO:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a Name for the user group.
3. In **Type**, select **RADIUS Single Sign-On (RSSO)**.
4. In **RADIUS Attribute Value**, enter the name of the RADIUS user group this local user group represents.
5. Select **OK**.

To define local user groups for RADIUS SSO:

This example creates an RSSO user group called RSSO-1 that is associated with RADIUS user group "student".

```
config user group
   edit RSSO-1
      set group-type rsso
      set sso-attribute-value student
```

```
end
```

Creating security policies

RADIUS SSO uses regular identity-based security policies. The RSSO user group you specify determines which users are permitted to use the policy. You can create multiple policies if user groups can have different UTM features enabled, different permitted services, schedules, and so on.

To create a security policy for RSSO - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Enter the following information.

Incoming Interface	as needed
Source Address	as needed
Source User(s)	Select the user groups you created for RSSO. See Defining local user groups for RADIUS SSO on page 591.
Outgoing Interface	as needed
Destination Address	all
Schedule	as needed
Service	as needed
Action	ACCEPT
Enable NAT	Selected
Security Profiles	Select security profiles appropriate for the user group.

4. Select **OK**.

   To ensure an RSSO-related policy is matched first, the policy should be placed higher in the security policy list than more general policies for the same interfaces.
5. Select **OK**.

To create a security policy for RSSO - CLI:

In this example, an internal network to Internet policy enables web access for members of a student group and activates the appropriate UTM profiles.

```
config firewall policy
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr all
      set dstaddr "all"
      set action accept
      set rsso enable
```

```
    set groups "RSSO-student"
    set schedule always
    set service HTTP HTTPS
    set nat enable
    set utm-status enable
    set av-profile students
    set webfilter-profile students
    set spamfilter-profile students
    set dlp-sensor default
    set ips-sensor default
    set application-list students
    set profile-protocol-options "default"
end
```

Example: webfiltering for student and teacher accounts

The following example uses RADIUS SSO to apply web filtering to students, but not to teachers. Assume that the RADIUS server is already configured to send RADIUS Start and Stop records to the FortiGate unit. There are two RADIUS user groups, **students** and **teachers**, recorded in the default attribute **Class**. The workstations are connected to port1, port2 connects to the RADIUS server, and port3 connects to the Internet.

Configure the student web filter profile:

1. Go to **Security Profiles > Web Filter** and select **Create New** (the "+" button).
2. Enter the following and select **OK**.

Name	student
Inspection Mode	Proxy
FortiGuard Categories	Enable. Right-click the **Potentially Liable** category and select **Block**. Repeat for **Adult/Mature Content** and **Security Risk**.

Create the RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.

Define local user groups associated with the RADIUS SSO user groups:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following and select **OK**.

Name	RSSO-students
Type	RADIUS Single Sign-On (RSSO)
RADIUS Attribute Value	students

3. Select **Create New**, enter the following and select **OK**.

Name	RSSO-teachers
Type	RADIUS Single Sign-On (RSSO)
RADIUS Attribute Value	teachers

Create a security policy for students:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter

Incoming Interface	port1
Source Address	all
Source User(s)	RSSO-students
Source Device Type	All
Outgoing Interface	port3
Destination Address	all
Schedule	always
Service	HTTP, HTTPS
Action	ACCEPT
NAT	ON
Security Profiles	Enable AntiVirus, Web Filter, IPS. In Web Filter, select the **student** profile.

3. Select **OK**.

Create a security policy for teachers:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter

Incoming Interface	port2
Source Address	all
Source User(s)	RSSO-teachers
Source Device Type	All
Outgoing Interface	port3

Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	ON
Security Profiles	Enable AntiVirus and IPS.

3. Select **OK**.

Monitoring authenticated users

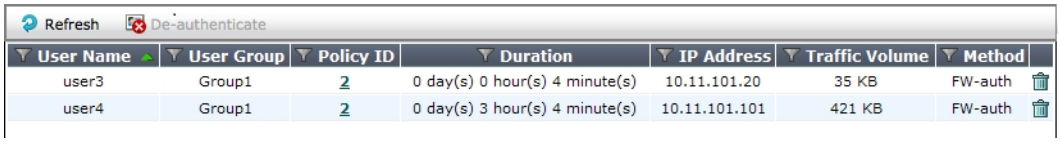
This section describes how to view lists of currently logged-in firewall and VPN users. It also describes how to disconnect users.

The following topics are included in this section:

- Monitoring firewall users
- Monitoring SSL VPN users
- Monitoring IPsec VPN users
- Monitoring users Quarantine

Monitoring firewall users

To monitor firewall users, go to **User & Device > Monitor > Firewall.**



You can de-authenticate a user by selecting the Delete icon for that entry.

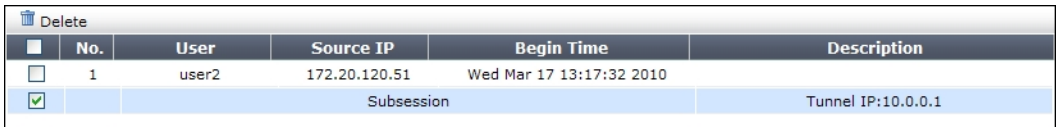
You can filter the list of displayed users by selecting the funnel icon for one of the column titles or selecting **Filter Settings**.

Optionally, you can de-authenticate multiple users by selecting them and then selecting **De-authenticate**.

Monitoring SSL VPN users

You can monitor web-mode and tunnel-mode SSL VPN users by username and IP address.

To monitor SSL VPN users, go to **VPN > Monitor > SSL-VPN Monitor**. To disconnect a user, select the user and then select the **Delete** icon.



The first line, listing the username and IP address, is present for a user with either a web-mode or tunnel-mode connection. The Subsession line is present only if the user has a tunnel mode connection. The **Description** column displays the virtual IP address assigned to the user's tunnel-mode connection.

For more information about SSL VPN, see the FortiOS Handbook SSL VPN guide.

To monitor SSL VPN users - CLI:

To list all of the SSL VPN sessions and their index numbers:

```
execute vpn sslvpn list
```

The output looks like this:

```
SSL-VPN Login Users:
 Index   User   Auth Type   Timeout         From      HTTPS in/out
 0       user1  1           256       172.20.120.51   0/0

SSL-VPN sessions:
 Index   User   Source IP        Tunnel/Dest IP
 0       user2  172.20.120.51    10.0.0.1
```

You can use the Index value in the following commands to disconnect user sessions:

To disconnect a tunnel-mode user

```
execute vpn sslvpn del-tunnel <index>
```

To disconnect a web-mode user

```
execute vpn sslvpn del-web <index>
```

You can also disconnect multiple users:

To disconnect all tunnel-mode SSL VPN users in this VDOM

```
execute vpn ssl del-all tunnel
```

To disconnect all SSL VPN users in this VDOM

```
execute vpn ssl del-all
```

Monitoring IPsec VPN users

To monitor IPsec VPN tunnels in the web-based manager, go to **VPN > Monitor > IPsec Monitor**. user names are available only for users who authenticate with XAuth.

You can close a tunnel by selecting the tunnel and right click to select **Bring Down**.

For more information, see the FortiOS Handbook IPsec VPN guide.

Monitoring users Quarantine

The User Quarantine list shows all IP addresses and interfaces blocked by NAC quarantine. The list also shows all IP addresses, authenticated users, senders, and interfaces blocked by Data Leak Prevention (DLP). The system administrator can selectively release users or interfaces from quarantine or configure quarantine to expire after a selected time period.

All sessions started by users or IP addresses on the User Quarantine list are blocked until the user or IP address is removed from the list. All sessions to an interface on the list are blocked until the interface is removed from the list.

You can configure NAC quarantine to add users or IP addresses to the User Quarantine list under the following conditions:

- **Users or IP addresses that originate attacks detected by IPS** - To quarantine users or IP addresses that originate attacks, enable and configure **Quarantine** in an IPS Filter.
- **Users or IP addresses that are quarantined by Data Leak Prevention** - In a DLP sensor select **Quarantine IP Address** as the action to take.

For more information, see FortiOS Handbook Security Profiles guide.

Users are viewed from **User & Device > Monitor > User Quarantine.**

Delete	Removes the selected user or IP address from the User Quarantine list.
Remove All	Removes all users and IP addresses from the User Quarantine list.
Search	Search the list for a particular IP address.
Source	The FortiGate function that caused the user or IP address to be added to the User Quarantine list: IPS or Data Leak Prevention.
Created	The date and time the user or IP address was added to the Banned User list.
Expires	The date and time the user or IP address will be automatically removed from the User Quarantine list. If **Expires** is **Indefinite**, you must manually remove the user or host from the list.

Examples and Troubleshooting

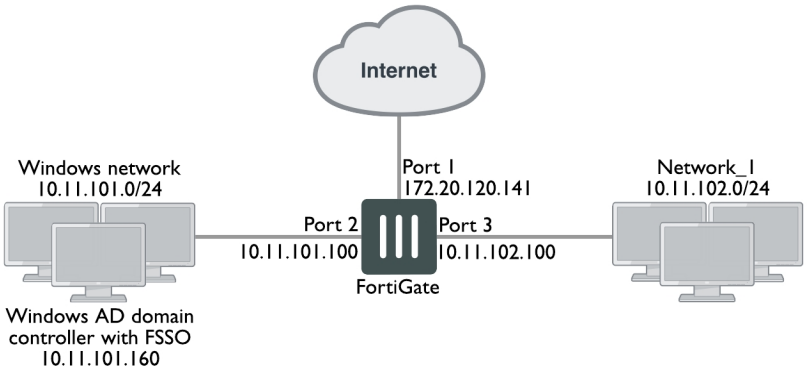
This chapter provides an example of a FortiGate unit providing authenticated access to the Internet for both Windows network users and local users.

The following topics are included in this section:

- Firewall authentication example
- LDAP Dial-in using member-attribute example
- RADIUS SSO example
- Troubleshooting

Firewall authentication example

Example configuration



Overview

In this example, there is a Windows network connected to Port 2 on the FortiGate unit and another LAN, Network_1, connected to Port 3.

All Windows network users authenticate when they logon to their network. Members of the Engineering and Sales groups can access the Internet without entering their authentication credentials again. The example assumes that the Fortinet Single Sign On (FSSO) has already been installed and configured on the domain controller.

LAN users who belong to the Internet_users group can access the Internet after entering their username and password to authenticate. This example shows only two users, User1 is authenticated by a password stored on the FortiGate unit, User2 is authenticated on an external authentication server. Both of these users are referred to as local users because the user account is created on the FortiGate unit.

Creating a locally-authenticated user account

User1 is authenticated by a password stored on the FortiGate unit. It is very simple to create this type of account.

To create a local user - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Follow the User Creation Wizard, entering the following information and then select **Create**:

User Type	Local User
User Name	User1
Password	hardtoguess
Email Address **SMS**	(optional)
Enable	Select.

To create a local user - CLI:

```
config user local
   edit user1
      set type password
      set passwd hardtoguess
   end
```

Creating a RADIUS-authenticated user account

To authenticate users using an external authentication server, you must first configure the FortiGate unit to access the server.

To configure the remote authentication server - web-based manager:

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information and select **OK**:

Name	OurRADIUSsrv
Primary Server Name/IP	10.11.101.15
Primary Server Secret	OurSecret
Authentication Scheme	Select **Use Default Authentication Scheme**.

To configure the remote authentication server - CLI:

```
config user radius
   edit OurRADIUSsrv
      set server 10.11.102.15
      set secret OurSecret
      set auth-type auto
   end
```

Creation of the user account is similar to the locally-authenticated account, except that you specify the RADIUS authentication server instead of the user's password.

To configure a remote user - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Follow the User Creation Wizard, entering the following information and then select **Create**:

User Type	Remote RADIUS User
User Name	User2
RADIUS server	OurRADIUSsrv
Email Address **SMS**	(optional)
Enable	Select

To configure a remote user - CLI:

```
config user local
   edit User2
      set name User2
      set type radius
      set radius-server OurRADIUSsrv
   end
```

Creating user groups

There are two user groups: an FSSO user group for FSSO users and a firewall user group for other users. It is not possible to combine these two types of users in the same user group.

Creating the FSSO user group

For this example, assume that FSSO has already been set up on the Windows network and that it uses Advanced mode, meaning that it uses LDAP to access user group information. You need to

- configure LDAP access to the Windows AD global catalog
- specify the collector agent that sends user logon information to the FortiGate unit
- select Windows user groups to monitor
- select and add the Engineering and Sales groups to an FSSO user group

To configure LDAP for FSSO - web-based manager:

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the following information:

Name	ADserver
Server Name / IP	10.11.101.160
Distinguished Name	dc=office,dc=example,dc=com

Bind Type	Regular
User DN	cn=FSSO_Admin,cn=users,dc=office,dc=example,dc=com
Password	set_a_secure_password

3. Leave other fields at their default values.
4. Select **OK**.

To configure LDAP for FSSO - CLI"

```
config user ldap
   edit "ADserver"
      set server "10.11.101.160"
      set dn "cn=users,dc=office,dc=example,dc=com"
      set type regular
      set username "cn=administrator,cn=users,dc=office,dc=example,dc=com"
      set password set_a_secure_password
   next
end
```

To specify the collector agent for FSSO - web-based manager

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New.**
2. Enter the following information:

Type	Fortinet Single Sign-On Agent
Name	WinGroups
Primary Agent IP/Name	10.11.101.160
Password	fortinet_canada
LDAP Server	ADserver

3. Select **Apply & Refresh**.

In a few minutes, the FortiGate unit downloads the list of user groups from the server.

To specify the collector agent for FSSO - CLI:

```
config user fsso
   edit "WinGroups"
      set ldap-server "ADserver"
      set password ENC
          G7GQV7NEqilCM9jKmVmJJFVvhQ2+wtNEe9T0iYA5Sa+EqT2J8zhOrbkJFDr0RmY3c4LaoXdsoBczA
          1dONmcGfthTxxwGsigzGpbJdC71spFlQYtj
      set server "10.11.101.160"
   end
```

To create the FSSO_Internet-users user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	FSSO_Internet_users
Type	Fortinet Single Sign-On (FSSO)
Members	Engineering, Sales

To create the FSSO_Internet-users user group - CLI:

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
   end
```

Creating the Firewall user group

The non-FSSO users need a user group too. In this example, only two users are shown, but additional members can be added easily.

To create the firewall user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	Internet_users
Type	Firewall
Members	User1, User2

To create the firewall user group - CLI:

```
config user group
   edit Internet_users
      set group-type firewall
      set member User1 User2
   end
```

Defining policy addresses

1. Go to **Policy & Objects > Objects > Addresses**.
2. Create the following addresses:

Address Name	Internal_net
Type	Subnet
Subnet / IP Range	10.11.102.0/24
Interface	Port 3

Address Name	Windows_net
Type	Subnet
Subnet / IP Range	10.11.101.0/24
Interface	Port 2

Creating security policies

Two security policies are needed: one for firewall group who connect through port3 and one for FSSO group who connect through port2.

To create a security policy for FSSO authentication - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	Port2
Source Address	Windows_net
Source User(s)	FSSO_Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	ON
Security Profiles	Optionally, enable security profiles.

3. Select OK.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr Windows_net
      set dstaddr all
      set action accept
      set groups FSSO_Internet_users
      set schedule always
      set service ANY
      set nat enable
   end
```

To create a security policy for local user authentication - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	Port3
Source Address	Internal_net
Source User(s)	Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	ON
Security Profiles	Optionally, enable security profiles.

3. Select **OK**.

To create a security policy for local user authentication - CLI

```
config firewall policy
   edit 0
      set srcintf port3
      set dstintf port1
      set srcaddr internal_net
      set dstaddr all
      set action accept
      set schedule always
      set groups Internet_users
      set service ANY
      set nat enable
   end
```

LDAP Dial-in using member-attribute example

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to set up a VPN connection simply based on an attribute that is set to TRUE, instead of based on their user group. In AD the "Allow Dialin" property is activated in the user properties, and this sets the `msNPAllowDialin` attribute to "TRUE".

This same procedure can be used for other member attributes, as your system requires.

To accomplish this with a FortiGate unit, member-attribute must be set. This can only be accomplished through the CLI - the option is not available through the web-based manager.

Before configuring the FortiGate unit, ensure the AD server has the `msNPAllowDialin` attribute set to "TRUE" for the users in question. If not, those users will not be able to authenticate.

To configure user LDAP member-attribute settings - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=fortilabanz,DC=com,DC=au"
      set type regular
      set username "fortigate@sample.com"
      set password ******
      set member-attr "msNPAllowDialin"
   next
end
```

To configure LDAP group settings - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
      config match
         edit 1
            set server-name "ldap"
            set group-name "TRUE"
         next
      end
   next
end
```

Once these settings are in place, users that are a member of the `ldap` user group will be able to authenticate.

To ensure your settings are correct, here is the sample output from a diag debug command that shows the authentication process.

When the "Allow Dial-in" attribute is set to "TRUE" the following will likely be in the output:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the attribute is not set but it is expected, the following will likely be in the output:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='FALSE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Failed group matching
```

The only difference between these two outputs is the last line which is either passed or failed based on if the member-attribute is set to the expected value or not.

RADIUS SSO example

A common RADIUS SSO topology involves a medium sized company network of users connecting to the Internet through the FortiGate unit, and authenticating with a RADIUS server. RADIUS SSO authentication was selected because it is fast and relatively easy to configure.

This section includes:

- Assumptions
- Topology
- Configuring RADIUS
- Configuring FortiGate regular and RADIUS SSO security policies
- Testing

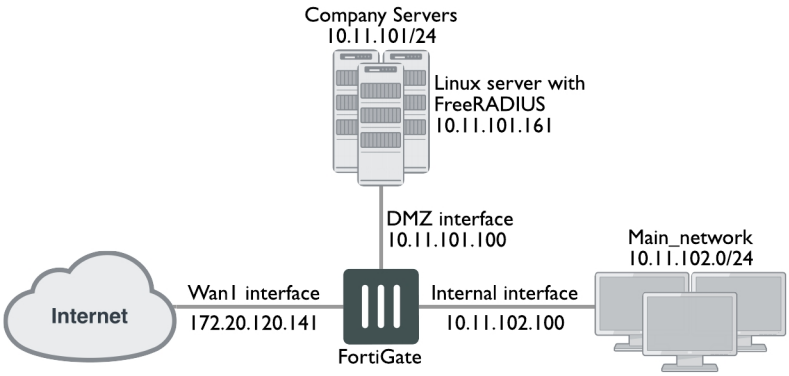
Assumptions

- VDOMs are not enabled
- The admin super_admin administrator account will be used for all FortiGate unit configuration.
- Any other devices on the network do not affect the topology of this example, and therefore are not included.
- Anywhere settings are not described, they are assumed to be default values.
- A RADIUS server is installed on a server or FortiAuthenticator unit and uses default attributes.
- BGP is used for any dynamic routing.
- Authentication event logging under Log&Report has been configured.

Topology

Example.com has an office with 20 users on the internal network. These users need access to the Internet to do their jobs. The office network is protected by a FortiGate-60C unit with access to the Internet through the wan1 interface, the user network on the internal interface, and all the servers are on the DMZ interface. This includes an Ubuntu Linux server running FreeRADIUS. For this example only two users will be configured — Pat Lee with an account name `plee`, or `plee@example.com`, and Kelly Green with an account name `kgreen`, or `kgreen@example.com`.

RADIUS SSO topology



Configuring RADIUS

Configuring RADIUS includes configuring the RADIUS server such as FreeRADIUS, a radius client on user's computers, and configuring users in the system. For this example the two users will be Pat Lee, and Kelly Green. They belong to a group called `exampledotcom_employees`. When it is all configured, the RADIUS daemon needs to started.

The users have a RADIUS client installed on their PCs that allows them to authenticate through the RADIUS server.

FreeRADIUS can be found on the freeradius.org website. For any problems installing FreeRADIUS, see the FreeRADIUS documentation.

Configuring FortiGate interfaces

Before configuring the RADIUS SSO security policy, configure FortiGate interfaces. This includes defining a DHCP server for the internal network as this type of network typically uses DHCP. The wan1 and dmz interfaces are assigned static IP addresses and do not need a DHCP server.

FortiGate interfaces used in this example

Interface	Subnet	Act as DHCP Server	Devices
wan1	172.20.120.141	No	Internet Service Provider
dmz	10.11.101.100	No	Servers, including RADIUS server
internal	10.11.102.100	Yes: x.x.x.110-.250	Internal user network

To configure FortiGate interfaces - web-based manager:

1. Go to **System > Network > Interfaces**.
2. Select wan1 to edit.
3. Enter the following information and select **OK**.

Alias	Internet
Addressing Mode	Manual
IP/Network Mask	172.20.120.141/255.255.255.0
Administrative Access	HTTPS, SSH
Enable DHCP Server	Not selected
Comments	Internet
Administrative Status	Up

4. Select dmz to edit.
5. Enter the following information and select **OK**.

Alias	Servers
Addressing Mode	Manual
IP/Network Mask	10.11.101.100/255.255.255.0
Administrative Access	HTTPS, SSH, PING, SNMP
Enable DHCP Server	Not selected
Listen for RADIUS Accounting Messages	Select
Comments	Servers
Administrative Status	Up

6. Select internal to edit.
7. Enter the following information and select **OK**.

Alias	Internal network
Addressing Mode	Manual
IP/Network Mask	10.11.102.100/255.255.255.0
Administrative Access	HTTPS, SSH, PING
Enable DHCP Server	Select
Address Range	10.11.102.110 - 10.11.102.250
Netmask	255.255.255.0
Default Gateway	Same as Interface IP
DNS Server	Same as System DNS
Comments	Internal network
Administrative Status	Up

Configuring a RADIUS SSO Agent on the FortiGate unit

To create a RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On Agent**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.
   The Single Sign-On agent is named RSSO_Agent.

Creating a RADIUS SSO user group

To define a local user group for RADIUS SSO:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a Name for the user group.
3. In **Type**, select **RADIUS Single Sign-On (RSSO)**.
4. In **RADIUS Attribute Value**, enter the name of the RADIUS user group this local user group represents.
5. Select **OK**.

Configuring FortiGate regular and RADIUS SSO security policies

With the RADIUS server and FortiGate interfaces configured, security policies can be configured. This includes both RADIUS SSO and regular policies, as well as addresses and address groups. All policies require NAT to be enabled.

Security policies required for RADIUS SSO

Seq. No.	From -> To	Type	Schedule	Description
1	internal -> wan1	RADIUS SSO	business hours	Authenticate outgoing user traffic.
2	internal -> wan1	regular	always	Allow essential network services and VoIP.
3	dmz -> wan1	regular	always	Allow servers to access Internet.
4	internal -> dmz	regular	always	Allow users to access servers.
5	any -> any	deny	always	Implicit policy denying all traffic that hasn't been matched.

The RADIUS SSO policy must be placed at the top of the policy list so it is matched first. The only exception to this is if you have a policy to deny access to a list of banned users. In this case, that policy must go at the top so the RADIUS SSO does not mistakenly match a banned user or IP address.

This section includes:

- Schedules, address groups, and services groups
- Configuring regular security policies
- Configuring RADIUS SSO security policy

Schedules, address groups, and services groups

This section lists the lists that need to be configured before security policies are created. Creating these lists is straight forward, so the essential information has been provided here but not step by step instructions. For more information on firewall related details, see

Schedules

Only one schedule needs to be configured — `business_hours`. This is a fairly standard Monday to Friday 8am to 5pm schedule, or whatever days and hours covers standard work hours at the company.

Address groups

The following address groups need to be configured before the security policies.

Address Group Name	Interface	Address range included
internal_network	internal	10.11.102.110 to 10.11.102.250
company_servers	dmz	10.11.101.110 to 10.11.101.250

Service groups

The following service groups need to be configured before the security policies. Note that the services listed are suggestions and may include more or less as required.

Service Group Name	Interface	Description of services to be included
essential_network_services	internal	Any network protocols required for normal network operation such as DNS, NTP, BGP.
essential_server_services	dmz	All the protocols required by the company servers such as BGP, HTTP, HTTPS, FTP, IMAP, POP3, SMTP, IKE, SQL, MYSQL, NTP, TRACEROUTE, SOCKs, and SNMP.
user_services	internal	Any protocols required by users HTTP, HTTP, FTP,

The following security policy configurations are basic and only include logging, and default AV and IPS.

Configuring regular security policies

Regular security policies allow or deny access for non-RADIUS SSO traffic. This is essential as there are network services—such as DNS, NTP, and FortiGuard—that require access to the Internet.

To configure regular security policies - web-based manager:

1. Go to **Policy & Objects > Policy > IP4**, and select **Create New**.
2. Enter the following information, and select **OK**.

Incoming Interface	Internal
Source Address	internal_network
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	essential_network_services
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	ON
Comments	Essential network services

3. Select **Create New**, enter the following information, and select **OK**.

Incoming Interface	dmz
Source Address	company_servers
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	essential_server_services
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	enable
Comments	Company servers accessing the Internet

4. Select **Create New**, enter the following information, and select **OK**.

Incoming Interface	Internal
Source Address	internal_network
Outgoing Interface	dmz
Destination Address	company_servers
Schedule	always
Service	all
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	enable
Comments	Access company servers

Configuring RADIUS SSO security policy

The RADIUS SSO policy allows access for members of specific RADIUS groups.

To configure RADIUS SSO security policy:

1. Go to **Policy & Objects > Policy > IP4**.
2. Select **Create New**.
3. Enter the following information:

Incoming Interface	Internal
Source Address	internal_network
Source User(s)	Select the user groups you created for RSSO.
Outgoing Interface	wan1
Destination Address	all
Schedule	business_hours
Service	ALL
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, WebFilter, IPS, and Email Filter. In each case, select the default profile.

4. Select **OK**.
5. To ensure an RSSO-related policy is matched first, the policy should be placed higher in the security policy list than more general policies for the same interfaces.
6. Select **OK**.

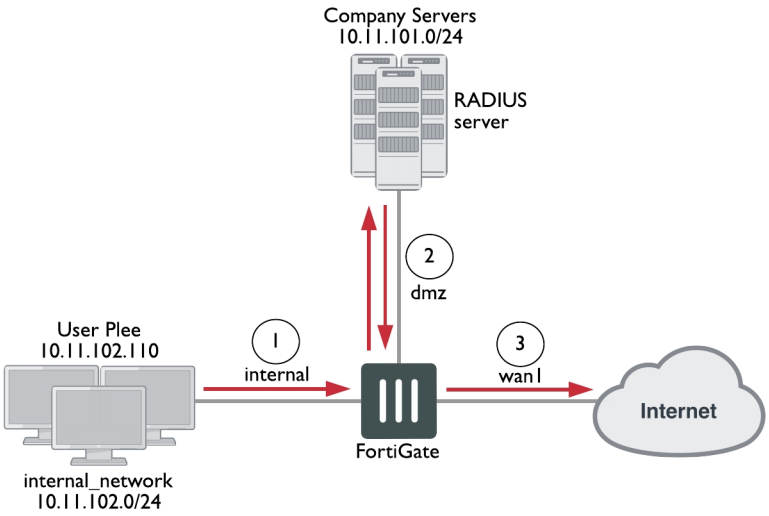
Testing

Once configured, a user only needs to log on to their PC using their RADIUS account. After that when they attempt to access an Internet website, the FortiGate unit will use their session information to get their RADIUS information. Once the user is verified, they are allowed access to the website.

To test the configuration perform the following steps:

1. Have user 'plee' logon to their PC, and try to access an Internet website.
2. The FortiGate unit will contact the RADUS server for user plee's information.
   Once confirmed, plee will have access to the website.
   Each step generates log entries that enable you to verify that each step was successful.
3. If a step is unsuccessful, confirm that your configuration is correct.

RADIUS SSO test



Troubleshooting

In the web-based manager, a good tool for troubleshooting is the packet counter column on the security policy page (**Policy > Policy**). This column displays the number of packets that have passed through this security policy. Its value when you are troubleshooting is that when you are testing your configuration (end to end connectivity, user authentication, policy use) watching the packet count for an increase confirms any other methods you may be using for troubleshooting. It provides the key of which policy is allowing the traffic, useful information if you expect a user to require authentication and it never happens. For more information about authentication security policies, see "Authentication in security policies".

This section addresses how to get more information from the CLI about users and user authentication attempts to help troubleshoot failed authentication attempts.

```
diag firewall iprope list
```

Shows the IP that the computer connected from. This is useful to confirm authorization and VPN settings.

`diag firewall iprope clear`
Clear all authorized users from the current list. Useful to force users to re-authenticate after system or group changes. However, this command may easily result in many users having to re-authenticate, so use carefully.

`diag rsso query ip`
`diag rsso query rsso-key`
Queries the RSSO database.

For more information on troubleshooting specific features, go to that section of this document. Most sections have troubleshooting information at the end of the section. In addition to that information, see the FortiOS Handbook Troubleshooting guide for general troubleshooting information.

Chapter 5 - Best Practices

Overview

This FortiGate Best Practices document is a collection of guidelines to ensure the most secure and reliable operation of FortiGate units in a customer environment. It is updated periodically as new issues are identified.

General Considerations

1. For security purposes, NAT mode is preferred because all of the internal or DMZ networks can have secure private addresses. NAT mode policies use network address translation to hide the addresses in a more secure zone from users in a less secure zone.
2. Use virtual domains (VDOMs) to group related interfaces or VLAN subinterfaces. Using VDOMs will partition networks and create added security by limiting the scope of threats.
3. Use Transparent mode when a network is complex and does not allow for changes in the IP addressing scheme.

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet Technical Support web site at http://support.fortinet.com.

You can also register Fortinet products and service contracts from http://support.fortinet.com and change your registration information at any time.

For information about our priority support hotline (live support), see http://support.fortinet.com.

When requesting technical support, please provide the following information:

- Your name, and your company's name and location
- Your email address and/or telephone number
- Your support contract number (if applicable)
- The product name and model number
- The product serial number (if applicable)
- The software or firmware version number
- A detailed description of the problem

Fortinet Knowledge Base

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Base. The knowledge base contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

System and performance

By implementing the following best practices for system and performance, you will ensure maximum efficiency of your FortiGate device. Be sure to read everything carefully, particularly the section that concerns shutting down the FortiGate system, in order to avoid potential hardware issues.

Performance

- Disable any management features you do not need. If you don't need SSH or SNMP, disable them. SSH also provides another possibility for would-be hackers to infiltrate your FortiGate unit.
- Put the most used firewall rules to the top of the interface list.
- Log only necessary traffic. The writing of logs, especially if to an internal hard disk, slows down performance.
- Enable only the required application inspections.
- Keep alert systems to a minimum. If you send logs to a syslog server, you may not need SNMP or email alerts, making for redundant processing.
- Establish scheduled FortiGuard updates at a reasonable rate. Daily updates occurring every 4-5 hours are sufficient for most situations. In more heavy-traffic situations, schedule updates for the evening when more bandwidth can be available.
- Keep security profiles to a minimum. If you do not need a profile on a firewall rule, do not include it.
- Keep VDOMs to a minimum. On low-end FortiGate units, avoid using them if possible.
- Avoid traffic shaping if you need maximum performance. Traffic shaping, by definition, slows down traffic.

Shutting down

Always shut down the FortiGate operating system properly before turning off the power switch to avoid potentially catastrophic hardware problems.

To power off the FortiGate unit - web-based manager:

1. Go to **System > Status**.
2. In the **System Resources** widget, select **Shutdown**.

To power off the FortiGate unit – CLI:

```
execute shutdown
```

Once this has been done, you can safely turn off the power switch or disconnect the power cables from the power supply.

Migration

Network administrators are often reluctant to change firewall vendors due to the perception that the migration process is difficult. Indeed, there is no point hiding the fact that moving to a new vendor requires careful consideration. But concern over the potential pain of migration should not stand in the way of adopting new security technologies. The purpose of this chapter is to describe the best practices for performing such migrations and ultimately to ease the migration process itself.

Information gathering

It is always best practice to perform a full network audit prior to any migration. This should include:

- Full back up of all security systems (including switches, routers) in case a back-out needs to be performed.
- Physical and logical network diagram with visual audit

Understanding exactly where cables run in the network and verifying they are all correctly labeled is essential to avoid mistakes and unnecessary downtime during the upgrade. Don't overlook simple things such as:

- Do I have enough spare interfaces on my switches?
- Do I have the right fiber (single/multi mode) and right connectors (LC, FC, MTRJ, SC, ST)?
- Do I have spare cables? (in the heat of the moment, it is a simple mistake to break an RJ-45 connector or damage a fiber)
- Do I have space in the rack for the new equipment?
- Do I have enough power sockets?

No matter how securely a FortiGate is configured in the network, it cannot help if it has been bypassed; visually checking where the device sits in the network in relation to other devices will ensure you are maintaining security and verify the network diagram is 'as built'. Details of all networks including subnet masks should be documented at this point to ensure that the replacement device is configured with the correct information.

Object and policy migration

Whilst we have suggested some level of manual review is included in the policy migration, it can be useful to be able to automatically migrate simply between another vendor's format and the FortiGate format. The FortiGate policy format is text based and can easily be cut and pasted into from other vendor formats however, responding to the high customer demand to migrate away from other vendors, Fortinet have released an automatic configuration migration tool at http://convert.fortinet.com to simplify this process. Supporting Cisco ACLs, PIX, ASA, Check Point, and Juniper, the Converter can securely upload and convert the policy into the Fortinet format.

Testing and validation

This is an important process and should be tested offline first wherever possible i.e. configure the policy in the lab or on a test network and verify that the required access permissions are being implemented. To really test the solution out, the FortiGate can be implemented on the live network with a different gateway IP and the selected user pointed to the new gateway. This allows a staged approach to migrating the new platform into the network ensuring that the process does not interrupt day to day operations.

Going live and obtaining feedback

If testing and validation is successful at this point, you can migrate to the new firewall either by switching IP's and removing the old devices or by changing the default gateway in DHCP. Once the firewall is in place, acceptance testing will of course need to be carried out and an iterative process of tuning undertaken to finalize the configuration.

Adding new services

The Fortinet solution will have a plethora of additional features compared to your previous vendor and it is very tempting to start switching them on but it is a good idea to wait and validate the new firewall as was previously configured before adding new functions as this simplifies testing and problem diagnosis. Finally complete the migration (don’t forget about the Plan Do Check Act Cycle) by adding any new services that were requested and learn about the multiple features you have available with the FortiGate appliance.

Environmental specifications

Keep the following environmental specifications in mind when installing and setting up your FortiGate unit.

- Operating temperature: 32 to 104°F (0 to 40°C). Temperatures may vary, depending on the FortiGate model.
- If you install the FortiGate unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature.
  Therefore, make sure to install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.
- Storage temperature: -13 to 158°F (-25 to 70°C). Temperatures may vary, depending on the FortiGate model.
- Humidity: 5 to 90% non-condensing.
- Air flow - For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.
- For free-standing installation, make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Depending on your device, the FortiGate may generate, use, and even radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Explosion is a serious risk if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Grounding

- Ensure the FortiGate unit is connected and properly grounded to a lightning and surge protector. WAN or LAN connections that enter the premises from outside the building should be connected to an Ethernet CAT5 (10/100 Mb/s) surge protector.
- Shielded Twisted Pair (STP) Ethernet cables should be used whenever possible rather than Unshielded Twisted Pair (UTP).
- Do not connect or disconnect cables during lightning activity to avoid damage to the FortiGate unit or personal injury.

Rack mounting

- **Elevated Operating Ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient.
  Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tmax) specified by the manufacturer.

- **Reduced Air Flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- **Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Firmware

Firmware upgrading and downgrading sounds pretty simple, anyone can do it, right? The mark of a professional is not that they can do something correctly, or even do it correctly over and over again. A professional works in such a way that, if anything goes wrong they are prepared and able to quickly get things back to normal. Firmware updates can go wrong just like anything else. So a real professional does things in a way that minimizes their risk and follows some best practices, as listed below.

Firmware change management

Consider the following five points when performing firmware upgrades, not only in FortiOS but in general. This applies to pretty much any change you have to do in a production environment.

Understanding the new version first

Before attempting any changes in production, first make sure you set up a laboratory where you can freely play with the new features, and understand them with enough time and no pressure. Read the Release Notes, Manuals, and other documentation like presentations, videos, or podcasts about the new version.

You are ready to explain the need for an upgrade once you understand:

- The differences and the enhancements between the new version and the previous version(s).
- The impact of the upgrade on customers and the users of the operating platform.
- The known limitations that might affect your environment.
- The potential risks when performing the upgrade.
- The licensing changes that may apply.

Never attempt to upgrade to a version you don't fully understand (both on features and known limitations), and on which you have no operational experience.

Have a valid reason to upgrade

The reason can NOT be “Because I want to have the latest version”. The reason has to be explained in terms of business, technical, and/or operational improvement.

Affirmative answers to the following questions are valid reasons to upgrade:

- Does the new version have a feature that helps to ensure compliance?
- Does the new version have an enhancement that allows 40% decrease (40% improvement) on the time to perform a certain operation?
- Does the new feature correct a known defect/bug found on a previous version that affects the company business/operations?
- Will the new version allow your organization to deploy new services that will help to gain new customers or increase loyalty of existing ones?
- Is the vendor cutting support for the version your organization is currently using?

If the best reason to upgrade is “Because the new features seem to be cool” or “Because I want to have the latest version”, a little more understanding and planning may be necessary.

Prepare an upgrade plan

If you choose to upgrade because you found a valid reason to do so, make sure you create a plan that covers business, technical, and operational aspects of the upgrade:

Business:

Proper planning and justification for an upgrade should be proportional to how critical the system is to the business.

- Make sure you can clearly articulate the benefits of the upgrade in business terms (time, money, and efficiency).
- Understand the business processes that will be affected by the change.
- Make sure the upgrade maintenance window is not close to a business-critical process (such as quarterly or monthly business closure).
- Obtain executive and operational approval for the maintenance window. The approval must come from the owners of ALL the systems/information affected by the upgrade, not only from those that own the system being upgraded. The approval must be done in a formal (written or e-mail) form.

Technical and operational:

- Re-read the Release Notes for the technology you are upgrading. Supported hardware models, upgrade paths, and known limitations should be clearly understood.
- Make sure your upgrade maintenance window does not overlap with any other maintenance window on your infrastructure.
- If you have any premium support offer (such as TAM, Premium Support), do a capacity planning exercise to ensure the new firmware/software version does not take more hardware resources than you currently have.
- Create a backup, whether or not you have scheduled backups. Create a new fresh backup.
- Obtain offline copies of both the currently installed firmware and the new version.
- Create a list of systems with inter-dependencies to the system you are upgrading. For example, if you are upgrading a FortiGate; understand the impact on any FortiAP, FortiAuthenticator, FortiToken, FortiManager, or FortiAnalyzer you have on your environment.
- Ensure you have a list of adjacent devices to the upgrading platform and have administrative access to them, just in case you need to do some troubleshooting. Are you upgrading FortiWeb? Make sure you can administratively access the Web Applications. Are you upgrading a FortiGate? Make sure you can administratively access the surrounding switches and routers.
- Have a step-by-step plan on how to perform and test the upgrade. You want to make sure you think of the worst situation before it happens, and have predefined courses of action, instead of thinking under pressure when something already went wrong.
- Define a set of tests (that include critical business applications that should be working) to make sure the upgrade went fine. If any test does not go well, define which ones mandate a rollback and which ones can be tolerated for further troubleshooting. This set of tests should be run before and after the upgrade to compare results, and they should be the same.
- Define a clear rollback plan. If something goes wrong with the upgrade or the tests, the rollback plan will help you get your environment back to a known and operational status. The plan must clearly state the conditions under which the rollback will be started.

- Declare configuration freezes. A little bit before and after the upgrade. The idea is to reduce the amount of variables to take into consideration if something goes wrong.
- Perform a “Quality Assurance” upgrade. Grab a copy of the production configuration, load it on a non-production box and execute the upgrade there to see if there are any issues on the process. Then adjust your plan according to the results you obtained.
- Have a list of information elements to be gathered if something goes wrong. This ensures that, even if the upgrade fails, you will collect enough information so you can troubleshoot the issue without needing to repeat the problem. Get help from TAC/Support departments if you need to check what else could be missing on your list.
- Define a test monitoring period after the change was completed. Even if the upgrade went smoothly, something could still go wrong. Make sure you monitor the upgraded system for at least one business cycle. Business cycles may be a week, a month, or a quarter, depending on your organization’s business priorities.

Execute the upgrade plan

Execution of an upgrade is just as key as planning.

Once you are performing the upgrade, the pressure will rise and stress might peak. This is why you should stick to the plan you created with a cool head.

Resist the temptation to take decisions while performing the upgrade, as your judgment will be clouded by the stress of the moment, even if a new decision seems to be “obvious” at such time. If your plan says you should rollback, then execute the rollback despite the potential “We-can-fix-this-very-quickly” mentality.

While performing the upgrade, make sure all the involved components are permanently monitored before, during, and after the upgrade, either via monitoring systems, SNMP alerts, or at least with tools like a ping. Critical resources like CPU, memory, network, and/or disk utilization must also be constantly monitored.

To avoid misunderstandings, when performing the tests for each critical application defined on the planning, make sure there are formal notifications on the results for each user area, service, system, and/or application tested.

Regardless if you have to rollback or not, if a problem occurs, make sure you gather as much information about the problem as possible, so you can later place a support ticket to find a solution.

Last but not least, document the upgrade:

- Enable your terminal emulation program to leave trace of all the commands executed and all the output generated. If you are performing steps via GUI, consider using a video capture tool to document it.
- Document any command or change performed over the adjacent/interdependent systems. Make sure they are acknowledged by the relevant administrators
- Document any deviations performed over the upgrade plan. This is planned-versus-actual.

Learn more about change management

Change Management and Change Control are huge knowledge areas in the field of Information Systems and Computer/Network Security.

This document is by no means a comprehensive list on what you should do when performing an upgrade, with either Fortinet or any other technology. It is merely a list of important things you should take into consideration when performing upgrades which are the result of years of experience dealing with changes on critical environments, as it is common that security devices are protecting critical applications and processes.

There are vast resources on the topic: books, public white papers, blog entries, etc. If you search the Internet for the “Change Control Best Practices” or “Change Management Best Practices” you will get many interesting documents.

Changes on production IT infrastructure are critical to the business. Make sure they play in your favor and not against you.

Performing a firmware upgrade

Upgrading a firewall is something that should be compared to upgrading the operating system on your computer. It’s not to be taken lightly! You want to make sure everything is backed up and you have some options available if things go awry. Assuming it all seems to work you also want a list of things to do in order to confirm everything is working properly. Finally, you need enough time to do it. All really simple stuff, but what does this mean in relation to upgrading your FortiGate? It means, you follow these simple steps:

1. **Backup and store old configuration (full configuration backup from CLI).**
   Digging into this a little, step 1 is easy to understand. Do a full backup of your old configuration. This is all part of your disaster recovery plan. If the upgrade fails in some way you need to make sure you can get the Firewall back up and running. The best way to do this is to get it back to a state where you know what the behavior was. For more information, refer to "Performing a configuration backup" on page 627.
2. **Have copy of old firmware available.**
   Step 2, is also part of your disaster recovery. If the upgrade fails you might be able to switch the active partition. But as a Professional, you need to be prepared for the worst case scenario where you can’t do that. Which means you’ll need your old firmware.
3. **Have disaster recovery option on standby -- especially if remote.**
   Step 3, is your plan for what to do in the event of a critical failure. As we’re talking FortiGate this means that your firewall doesn’t come back after the upgrade. What this means is that you need to be able to get to the console port in order to find out why. Maybe it’s DHCP and the IP changed, maybe the OS is corrupt, who knows? Get to the console and find out.
   There could be a simple fix. If there’s not, then be prepared for a format and TFTP reload.
4. **Read the release notes, including the upgrade path and bug information.**
   Step 4, READ THE RELEASE NOTES. They contain all kinds of information, known bugs, fixed bugs even upgrade issues like lost configuration settings. Not all upgrade information is ever contained in any products release notes. That does not mean they are devoid of good/useful information. Read them, digest them, then a few days later read them again.
5. **Double check everything.**
   Step 5, do a double check of everything. Is your TFTP server working, does your console connection function, is there anything in the release notes that could impact your upgrade procedure, do you have your configuration backed up? Make sure you’ve done everything.
6. **Upgrade.**
   Step 6, do the upgrade. Doing an upgrade doesn’t take very long, a few minutes (less a lot of times) but make sure you schedule enough time for it. At the end of the day an upgrade can succeed or fail. If it succeeds you want some time to check/confirm that any important features you have are working (VPNs etc). If it fails you’ll need time to sort things out.

Performing a firmware downgrade

Just like upgrading, you need to make sure it's done properly. While similar, the steps are somewhat different since there are other pitfalls in this case.

1. **Locate pre-upgrade configuration file.**
   Step 1 is very important. This is why, when you upgrade you make a backup of your old configuration and save it. If you don't, then you'll need to rebuild manually.
2. **Have copy of old firmware available.**
   Step 2 is fairly obvious. Even with devices that have multiple partitions and your downgrade process is simply going to be to switch the active partition, this could go wrong. In which case, you may be without Internet access. A professional has a plan for when things go wrong.
3. **Have disaster recovery option on standby -- especially if remote.**
   Step 3 is no different from before. Hopefully you don't need to format the unit, but be prepared for that, just in case.
4. **Read the release notes -- is a downgrade possible, or necessary?**
   Step 4, once again, is to READ THE RELEASE NOTES. In this case, you will need to do this for the version you are on, and the version you are downgrading too, and everything in between (if you are going back multiple major releases or patches). Maybe the OS switched from 32 to 64 bits somewhere between the two firmware releases. In order to make sure you don't get nailed by something like that you need to check the upgrade and downgrade information in every major release and patch, as it may have a direct impact on your options.
5. **Double check everything.**
6. **Downgrade -- all settings, except those needed for access, are lost.**
   Step 5 and 6 are the same as before. Double check everything, then downgrade.
7. **Restore pre-upgrade configuration.**
   Step 7 is new. Obviously most settings are lost when you downgrade so in order to get back up and running you will need to restore your old configuration file.

Performing a configuration backup

Once you configure the FortiGate unit and it is working correctly, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate unit to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it.

It is also recommended that once any further changes are made that you backup the configuration immediately, to ensure you have the most current configuration available. Also, ensure you backup the configuration before upgrading the FortiGate unit's firmware. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site.The latter two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate unit or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

To back up the FortiGate configuration - web-based manager:

1. Go to **System > Dashboard > Status**.
2. On the **System Information** widget, select **Backup** next to **System Configuration**.
3. Select to backup to your **Local PC** or to a **USB Disk**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
4. If VDOMs are enabled, select to backup the entire FortiGate configuration (**Full Config**) or only a specific VDOM configuration (**VDOM Config**).
5. If backing up a VDOM configuration, select the VDOM name from the list.
6. Select **Encrypt configuration file**.
   Encryption must be enabled on the backup file to back up VPN certificates.
7. Enter a password and enter it again to confirm it. You will need this password to restore the file.
8. Select **Backup**.
9. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

To back up the FortiGate configuration - CLI:

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP (note that port number, username are optional depending on the FTP site)…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>]
    [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
   edit <vdom_name>
```

Backing up a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. SCP is enabled using the CLI commands:

```
config system global
   set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
   set admin-scp enable
end
```

```
config vdom
   edit <vdom_name>
```

Security Profiles (AV, Web Filtering etc.)

Infection can come from many sources and have many different effects. Because of this, there is no single means to effectively protect your network. Instead, you can best protect your network with the various UTM tools your FortiGate unit offers.

Firewall

- Be careful when disabling or deleting firewall settings. Changes that you make to the firewall configuration using the GUI or CLI are saved and activated immediately.
- Arrange firewall policies in the policy list from more specific to more general. The firewall searches for a matching policy starting from the top of the policy list and working down. For example, a very general policy matches all connection attempts. When you create exceptions to a general policy, you must add them to the policy list above the general policy.
- Avoid using the All selection for the source and destination addresses. Use addresses or address groups.
- If you remove all policies from the firewall, there are no policy matches and all connections are dropped.
- If possible, avoid port ranges on services for security reasons.
- The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address. Do not use Any as a service. Use subnets or specific IP addresses for source and destination addresses and use individual services or service groups.
- Use a 32-bit subnet mask when creating a single host address (for example, 255.255.255.255).
- Use logging on a policy only when necessary and be aware of the performance impact. For example, you may want to log all dropped connections but can choose to use this sparingly by sampling traffic data rather than have it continually storing log information you may not use.
- It is possible to use security policies based on 'any' interface. However, for better granularity and stricter security, explicit interfaces are recommended.
- Use the comment field to input management data, for example: who requested the rule, who authorized it, etc.
- Avoid FQDN addresses if possible, unless they are internal. It can cause a performance impact on DNS queries and security impact from DNS spoofing.
- For non vlan interfaces, use zones (even if you have only one single interface for members) to allow:
  - An explicit name of the interface to use in security policies ('internal' is more explicit than 'port10').
  - A split between the physical port and its function to allow port remapping (for instance moving from a 1G interface to a 10G interface) or to facilitate configuration translation, as performed during hardware upgrades.

Security

- Use NTP to synchronize time on the FortiGate and the core network systems, such as email servers, web servers, and logging services.
- Enable log rules to match corporate policy. For example, log administration authentication events and access to systems from untrusted interfaces.
- Minimize adhoc changes to live systems, if possible, to minimize interruptions to the network. When not possible, create backup configurations and implement sound audit systems using FortiAnalyzer and FortiManager.
- If you only need to allow access to a system on a specific port, limit the access by creating the strictest rule possible.

Authentication

- You must add a valid user group to activate the Authentication check box on the firewall policy configuration page.
- Users can authenticate with the firewall using HTTP or FTP. For users to be able to authenticate, you must add an HTTP or FTP policy that is configured for authentication.

Antivirus

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure you receive antivirus signature updates as soon as they are available.
- To ensure that all AV push updates occur, ensure you have an AV profile enabled in a security policy.
- Enable only the protocols you need to scan. If you have antivirus scans occurring on the SMTP server, or use FortiMail, it is redundant to have scanning occur on the FortiGate unit as well.
- Reduce the maximum file size to be scanned. Viruses usually travel in small files of around 1 to 2 megabytes.
- Do not quarantine files unless you regularly monitor and review them. This is otherwise a waste of space and impacts performance.
- Examine antivirus reports and log messages periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.

Antispam

- If possible use, a FortiMail unit. The antispam engines are more robust.
- Use fast DNS servers.
- Use specific security profiles for the rule that will use antispam.
- DNS checks may cause false positive with HELO DNS lookup.
- Content analysis (banned words) may impose performance overhead.

Intrusion Prevention System (IPS)

Your FortiGate's IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions. Refer to the following list of best practices regarding IPS.

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive IPS signature updates as soon as they are available.
- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to Block.
- Create and use security profiles with specific signatures and anomalies you need per-interface and per-rule.
- Do not use predefined or generic profiles. While these profiles are convenient to supply immediate protection, you should create profiles to suit your network environment.

- If you do use the default profiles, reduce the IPS signatures/anomalies enabled in the profile to conserve processing time and memory.
- If you are going to enable anomalies, make sure you tune thresholds according to your environment.
- If you need protection, but not audit information, disable the logging option.
- Tune the IP-protocol parameter accordingly.

Blocking Skype using CLI options for improved detection

If you want to identify or block Skype sessions, use the following CLI command with your FortiGate's public IP address to improve detection (FortiOS 4.3.12+ and 5.0.2+):

```
config ips global
   set skype-client-public-ipaddr 198.51.100.0,203.0.113.0
end
```

Note that the above syntax is configured using multiple public IP addresses, where a single public IP address may suffice depending on your network configuration.

Email filter

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine.

- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to the FortiGuard AntiSpam Service.

URL filtering

Best practices for URL filtering can be divided into four categories: flow-based versus proxy based filtering; local category/rating feature; URL filter 'Exempt' action; and Deep Scan.

Flow-based versus proxy-based

Try to avoid mixing flow-based and proxy-based features in the same profile if you are not using IPS or Application Control.

Local category/rating feature

Local categories and local rating features consume a large amount of CPU resources, so use this features as little as possible. It is better to use Local categories instead of using the 'override' feature, since the 'override' feature is more complicated and more difficult to troubleshoot.

URL filter 'Exempt' action

When using the URL filter 'Exempt' option, all scans (including antivirus) are bypassed by default, so use this option only for trusted sites.

Configuration notes: You need to configure 'Exempt' actions in the URL filter if you want to bypass the FortiGuard Web Filter.You can configure which particular inspection(s) you want to bypass using the `set exempt` command in `config webfilter urlfilter`.

Deep Scan

The 'Deep Scan' feature is much heavier on resources than 'HTTPS URL Scan Only'. Deep Scan is much more accurate, since many sites (such as various Google applications) cannot be scanned separately without deep scanning enabled.

Note: If you configre Deep Scan in the SSL profile and then configure 'Enable HTTPS URL Scan Only' in the web filter profile, then Deep Scan is not performed.

Web filtering

FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous

Patch management

When vulnerabilities are discovered in software, the software vendors release updates that fix these problems. Keeping your software and operating system up-to-date is a vital step to prevent infection and defend against attacks.

- Follow the latest advisories and reports on the FortiGuard webpage.
- Apply updates to all software as the updates become available.
- FortiGuard Vulnerability Management can help identify security weaknesses in your network. This subscription service is available through FortiScan and FortiAnalyzer units.
- Apply firmware updates to your FortiGate unit as they are released.
- Subscribe to FortiGuard AntiVirus and IPS services, so that AntiVirus and IPS scanning engines are automatically updated when new version are released.

Policy configuration

Configuring the FortiGate unit with an 'allow all' traffic policy is very undesirable. While this does greatly simplify the configuration, it is less secure. As a security measure, it is best practice for the policy rulebase to 'deny' by default, and not the other way around.

Policy configuration changes

On a heavy-loaded system, plan configuration changes during low usage periods in order to minimize impact on CPU usage and established sessions. In this scenario, it is considered a best practice to de-accelerate the hardware-accelerated sessions.

You can configure de-accelerated behaviour on hardware-accelerated sessions using CLI commands to control how the processor manages policy configuration changes. The following CLI commands are to be used:

```
config system settings
   set firewall-session-dirty { check-all | check-new | check-policy-option }
end
```

where you want the following to be true:

`check-all`	CPU flushes all current sessions and re-evaluates them. This is the default option.
`check-new`	CPU keeps existing sessions and applies policy changes to new sessions only. This reduces CPU load and the possibility of packet loss.
`check-policy-option`	Use the option selected in the `firewall-session-dirty` field of the firewall policy (`check-all` or `check-new`, as above, but per policy).

Policy whitelisting

- Allow only the necessary inbound and outbound traffic.
- If possible, limit traffic to specific addresses or subnets. This allows the FortiGate unit to drop traffic to and from unexpected addresses.

IPS and DoS policies

- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to Block.
- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to Block.
- DoS attacks are launched against vulnerabilities. Maintain a FortiGuard IPS subscription to ensure your FortiGate unit automatically receives new and updated IPS signatures as they are released.
- Use and configure DoS policies to appropriate levels based on your network traffic and topology. This will help drop traffic if an abnormal amount is received. The key is to set a good threshold. The threshold defines the maximum number of sessions/packets per second of normal traffic. If the threshold is exceeded, the action is triggered. Threshold defaults are general recommendations, but your network may require very different values. One way to find the correct values for your environment is to set the action to Pass and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your system will be from DoS attacks, but your system will also be more likely to generate false alarms.

Networking

When configuring your network, ensure that there is no 'back door' access to the protected network. For example, if there is a wireless access point, it must be appropriately protected with password and encryption.

Be sure to also maintain an up-to-date network diagram which includes IP addressing, cabling, and network elements.

Routing configuration

- Always configure a default route.
- Add blackhole routes for subnets reachable using VPN tunnels. This ensures that if a VPN tunnel goes down, traffic is not mistakingly routed to the Internet unencrypted.

Policy routing

Keep the number of policy routes to a minimum to optimize performance in route lookup and to simplify troubleshooting.

Dynamic routing

- Select a Router ID that matches an IP assigned to an interface. This avoids the likelihood of having two devices with the same router ID.
- For routing over an IPsec tunnel, assign IP addresses to both ends of the tunnel.

Advanced routing

Use the following best practices for advanced routing when dealing with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

Border Gateway Protocol (BGP)

If you are using BGP, it is recommended that you enable soft-reconfiguration. This has two benefits:

- It allows you to perform 'soft clear' of peers after a change is made to a BGP policy.
- It provides greater visibility into the specific prefixes learned from each neighbor.

Leave soft-reconfiguration disabled if your FortiGate does not have much unused memory. Soft-reconfiguration requires keeping separate copies of prefixes received and advertised, in addition to the local BGP database.

Open Shortest Path First (OSPF)

- Avoid use of passive interfaces wherever possible.
- Avoid use of virtual links to connect areas. All areas should be designed to connect directly to the backbone area.
- Ensure that all backbone routers have a minimum of two peering connections to other backbone neighbors.
- An entire OSPF domain should be under common administration.

Network Address Translation (NAT)

- Beware of misconfiguring the IP Pool range. Double-check the start and end IPs of each IP pool. The IP pool should not overlap with addresses assigned to FortiGate interfaces or to any hosts on directly connected networks.
- If you have internal and external users accessing the same servers, use split DNS to offer an internal IP to internal users so that they don't have to use the external-facing VIP.

Configuring NAT

Do not enable NAT for inbound traffic unless it is required by an application. If, for example, NAT is enabled for inbound SMTP traffic, the SMTP server might act as an open relay.

Transparent Mode

- Do not connect two ports to the same VLAN on a switch or to the same hub. Some Layer 2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN.
- If you operate multiple VLANs on your FortiGate unit, assign each VLAN id to its own forwarding domain to ensure that the scope of the broadcast does not extend beyond the VLAN it originated in.

To protect against Layer 2 loops:

- Enable `stpforward` on all interfaces.
- Use separate VDOMs for production traffic (TP mode VDOM) and management traffic (NAT/Route mode VDOM).
- Only place those interfaces used for production in the TP mode VDOM. Place all other interfaces in the NAT/Route mode VDOM. This protects against potential Layer 2 loops.

Using Virtual IPs (VIPs)

- Use the external IP of 0.0.0.0 when creating a VIP for a FortiGate unit where the external interface IP address is dynamically assigned.
- Be sure to select the correct external interface when creating a new virtual IP (VIP). The external interface should be set to the interface at which the FortiGate unit receives connection requests from external networks.

FGCP High Availability

Fortinet suggests the following practices related to high availability:

- Use Active-Active HA to distribute TCP and UTM sessions among multiple cluster units. An active-active cluster may have higher throughput than a standalone FortiGate unit or than an active-passive cluster.
- Use a different host name on each FortiGate unit when configuring an HA cluster. Fewer steps are required to add host names to each cluster unit before configuring HA and forming a cluster.
- Consider adding an Alias to the interfaces used for the HA heartbeat so that you always get a reminder about what these interfaces are being used for.
- Enabling `load-balance-all` can increase device and network load since more traffic is load-balanced. This may be appropriate for use in a deployment using the firewall capabilities of the FortiGate unit and IPS but no other content inspection.
- An advantage of using session pickup is that non-content inspection sessions will be picked up by the new primary unit after a failover. The disadvantage is that the cluster generates more heartbeat traffic to support session pickup as a larger portion of the session table must be synchronized. Session pickup should be configured only when required and is not recommended for use with SOHO FortiGate models. Session pickup should only be used if the primary heartbeat link is dedicated (otherwise the additional HA heartbeat traffic could affect network performance).
- If session pickup is not selected, after a device or link failover all sessions are briefly interrupted and must be re-established at the application level after the cluster renegotiates. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Users downloading large files may have to restart their download after a failover. Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.
- If you need to enable session pickup, consider enabling session pickup delay to improve performance by reducing the number of sessions that are synchronized.
- Consider using the `session-sync-dev` option to move session synchronization traffic off the HA heartbeat link to one or more dedicated session synchronization interfaces.
- To avoid unpredictable results, when you connect a switch to multiple redundant or aggregate interfaces in an active-passive cluster you should configure separate redundant or aggregate interfaces on the switch; one for each cluster unit.
- Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. Alert messages about cluster failovers may help find and diagnose network problems quickly and efficiently.

Heartbeat interfaces

Fortinet suggests the following practices related to heartbeat interfaces:

Do not use a FortiGate switch port for the HA heartbeat traffic. This configuration is not supported.

- For clusters of two FortiGate units, as much as possible, heartbeat interfaces should be directly connected using patch cables (without involving other network equipment such as switches). If switches have to be used they should not be used for other network traffic that could flood the switches and cause heartbeat delays.

  - If you cannot use a dedicated switch, the use of a dedicated VLAN can help limit the broadcast domain to protect the heartbeat traffic and the bandwidth it creates.
- For clusters of three or four FortiGate units, use switches to connect heartbeat interfaces. The corresponding heartbeat interface of each FortiGate unit in the cluster must be connected to the same switch. For improved redundancy use a different switch for each heartbeat interface. In that way if the switch connecting one of the heartbeat interfaces fails or is unplugged, heartbeat traffic can continue on the other heartbeat interfaces and switch.
- Isolate heartbeat interfaces from user networks. Heartbeat packets contain sensitive cluster configuration information and can consume a considerable amount of network bandwidth. If the cluster consists of two FortiGate units, connect the heartbeat interfaces directly using a crossover cable or a regular Ethernet cable. For clusters with more than two units, connect heartbeat interfaces to a separate switch that is not connected to any network.
- If heartbeat traffic cannot be isolated from user networks, enable heartbeat message encryption and authentication to protect cluster information. See Enabling or disabling HA heartbeat encryption and authentication.
- Configure and connect redundant heartbeat interfaces so that if one heartbeat interface fails or becomes disconnected, HA heartbeat traffic can continue to be transmitted using the backup heartbeat interface. If heartbeat communication fails, all cluster members will think they are the primary unit resulting in multiple devices on the network with the same IP addresses and MAC addresses (condition referred to as *Split Brain*) and communication will be disrupted until heartbeat communication can be reestablished.
- Do not monitor dedicated heartbeat interfaces; monitor those interfaces whose failure should trigger a device failover.
- Where possible at least one heartbeat interface should not be connected to an NPx processor to avoid NPx-related problems from affecting heartbeat traffic.

Interface monitoring (port monitoring)

Fortinet suggests the following practices related to interface monitoring (also called port monitoring):

- Wait until a cluster is up and running and all interfaces are connected before enabling interface monitoring. A monitored interface can easily become disconnected during initial setup and cause failovers to occur before the cluster is fully configured and tested.
- Monitor interfaces connected to networks that process high priority traffic so that the cluster maintains connections to these networks if a failure occurs.
- Avoid configuring interface monitoring for all interfaces.
- Supplement interface monitoring with remote link failover. Configure remote link failover to maintain packet flow if a link not directly connected to a cluster unit (for example, between a switch connected to a cluster interface and the network) fails. See Remote link failover.

WAN Optimization

WAN Optimization features require significant memory resources and generate a high amount of I/O on disk. Before enabling WAN Optimization, ensure that the memory usage is not too high. If possible, avoid other disk-intensive features such as heavy traffic logging on the same disk as the one configured for WAN Optimization needs.

In general, it is preferable to enable the Transparent Mode checkbox and ensure that routing between the two endpoints is acceptable. Some protocols may not work well without enabling Transparent Mode.

Other best practices for utilizing the WAN Optimization feature follow.

Sharing the WAN Opt. tunnel for traffic of the same nature

WAN optimization tunnel sharing is recommended for similar types of WAN optimization traffic (such as CIFS traffic from different servers). However, tunnel sharing for different types of traffic is not recommended. For example, aggressive and non-aggressive protocols should not share the same tunnel.

Ordering WAN Opt. rules appropriately

- Precise, port specific WAN Optimization rules should be at the top of the list.
- Generic rules, such as overall TCP, should be at the bottom of the list.

Avoiding mixing protocols in a WAN Opt. tunnel

Different protocols may be more or less talkative or interactive . Mixing protocols in a tunnel may result in a delay for some of them. It is recommended to define protocol specific wan-optimization rules and restrict the ports to the necessary ones only for performance reasons.

Setting correct configuration options for CIFS WAN Opt.

Ensure that the WAN Optimization rules cover TCP ports 139 and 445 (on the same or two different rules). Also ensure that Transparent Mode is selected.

Setting correct configuration options for MAPI WAN Opt.

For MAPI WAN Optimization, only specify a rule with TCP port 135 (unless the MAPI control port is configured differently). Derived data sessions using other random ports will be handled by the CIFS wan-optimization daemon even with only the control port configured.

Testing WAN Opt. in a lab

- Ensure that WAN emulators are used to simulate the WAN. If no WAN emulator is used, it is expected to have better results without WAN Optimization than with WAN Optimization.
- To test the difference between cold transfers (first-time transfers) and warm transfers, it is recommended to generate a random file of the cold transfer to ensure that the test is the first time that the file has been seen.

Regarding byte compression and type of file

Enabling byte compression on file transfers already compressed (.jpeg files, compressed archive, etc.) won't provide any performance increase and could be seen as a misuse of CPU resources.

Regarding network address translation (NAT)

Selecting the NAT feature in a security policy does not have any influence on WAN Optimization traffic.

High Availability

There is no benefit to using active-active mode, so for pure WAN Optimization needs, use active-passive mode. Refer to the FGCP High Availability section for other best practices related to HA.

Authentication with specific peers

Configure WAN optimization authentication with specific peers. Accepting any peer is not recommended as this can be less secure.

Virtual Domains (VDOMs)

VDOMs can provide separate firewall policies and, in NAT/Route mode, completely separate configurations for routing and VPN services for each connected network or organization. This section provides a list of best practices for configuring VDOMs.

Per-VDOM resource settings

While Global resources apply to resources shared by the whole FortiGate unit, per-VDOM resources are specific to only one Virtual Domain.

By default all the per-VDOM resource settings are set to no limits. This means that any single VDOM can use up all the resources of the entire FortiGate unit if it needs to do so. This would starve the other VDOMs for resources to the point where they would be unable to function. For this reason, it is recommended that you set some maximums on resources that are most vital to your customers.

Virtual domains in NAT/Route mode

Once you have enabled virtual domains and created one or more VDOMs, you need to configure them. It is recommended that you perform the following tasks in the order given (while you may not require all for your network topology):

1. Change the management virtual domain.
2. Configure FortiGate interfaces in a NAT/Route VDOM.
3. Configure VDOM routing.
4. Configure security policies for NAT/Route VDOMs.
5. Configure UTM profiles for NAT/Route VDOMs.
6. Test the configuration.

Virtual clustering

If you decide to disable override for clurstering, as a result of persistent renegotiating, you should disable it for both cluster units.

Explicit proxy

- For explicit proxies, when configuring limits on the number of concurrent users, you need to allow for the number of users based on their authentication method. Otherwise you may run out of user resources prematurely.
- Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSSO, local database etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.
- For all other situations, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.
- Set the explicit web proxy and explicit FTP proxy Default Firewall Policy Action to Deny. This means that a firewall policy is required to use these explicit proxies, allowing you to control access and impose security features.
- Do not enable the explicit web or FTP proxy on an interface connected to the Internet. This is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address. If you must enable the proxy on such an interface make sure authentication is required to use the proxy.

Wireless

The following section contains a list of best practices for wireless network configurations with regard to encryption and authentication, geographic location, network planning, power usage, client load balancing, local bridging, SSIDs, and the use of static IPs.

Encryption and authentication

It is best practice to always enable the strongest user authentication and encryption method that your client supports. Fortinet recommends the following security, in order of strongest to weakest:

- WPA2 - Enterprise 802.1x/EAP - Personal pre-shared key (8-63 characters)
- WPA - Enterprise 802.1x/EAP - Personal pre-shared key (8-63 characters)
- WEP128 - 26 Hexadecimal digit key
- WEP64 - 10 Hexadecimal digit key
- None - Open system

Geographic location

Ensure that the FortiGate wireless controller is configured for your geographic location. This ensures that the available radio channels and radio power are in compliance with the regulations in your region.

The maximum allowed transmitter power and permitted radio channels for Wi-Fi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, you need to set your location before you begin configuring wireless networks.

The location setting can only be changed from CLI. To change the country to France, for example, enter the following:

```
config wireless-controller setting
   set country FR
end
```

To see the list of country codes, enter a question mark ('?') in place of the country code.

Using an incorrect geographic location is a common error that can lead to unpredicable results on the client side.

Network planning

It is recommended that you perform a proper site survey prior positioning the wireless access point. In order to evaluate the coverage area environment, the following criteria must be taken into account:

- Size of coverage area
- Bandwidth required
- Client wireless capabilities

After completing a RF site survey, you'll have a good idea of the number and location of access points needed to provide users with adequate coverage and performance.

However, prior to installing the access points, be sure to determine the RF channel(s) you plan to use. This will ensure that users can roam throughout the facility with substantial performance.

To avoid co-channel interference, adjacent Wi-Fi APs must be configured to use non-overlapping channels. Otherwise, you'll find poor performance will degrade because of interference between access points.

It is recommended to statically configure the non-overlapping channels on every access point, using one Custom AP profile per AP (or group of APs). If static configuration cannot be used, the FortiOS Wi-Fi Controller includes the Automatic Radio Resource Provisioning (ARRP) feature.

Lowering the power level to reduce RF interference

Relevant Product(s): FortiAP

Reducing power reduces unwanted coverage and potential interference to other WLANs. Areas of unwanted coverage are a potential security risk. If possible, reduce the transmitter power of your wireless access point so that the signal is not available beyond the areas where it is needed. Auto Tx Power Control can be enabled to automatically adjust the transmit power.

In cases where customers complain about slow wireless traffic through a FortiAP, it might be necessary to try to reduce the possibility of RF interference. It is best practice not to locate FortiAPs near steel beams or other interfering materials. You can try using a wireless sniffer tool to collect the wireless packets and then analyze the extent of air interference.

A common mistake is spacing FortiAPs based upon the 5Ghz radio frequency. The 2.4Ghz signal travels further.

You have two options when confronted with slow wireless traffic through a FortiAP:

Option #1: Reducing transmit power

Perform a speed test and record the results. Set one of the radios on a FortiAP to be in dedicated monitoring mode. Then observe how many APs are detected. If the number of APs is too high (i.e., greater than 20), try reducing the transmit power in the WTP profile for the FortiAPs until the number of dedicated APs has dropped significantly.

Repeat the speed test.

Option #2: Ensuring that VAPs are distributed over the available channels

No built-in tools are available to measure RF interference directly. However, FortiOS 5.0 does allow for automatic power adjustment, which should minimize the occurrence of RF interference.

Wireless client load balancing

Wireless load balancing allows your wireless network to more efficiently distribute wireless traffic among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- **Access Point Hand-off** - The wireless controller signals a client to switch to another access point.
- **Frequency Hand-off** - The wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Local bridging

Whenever possible, use local bridging to offload the CAPWAP tunnel. Note that in this case, Wi-Fi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN. The vlan ID can only be configured

from the CLI:

```
config wireless-controller vap
   edit "vaplocalbridge"
      set vdom "root"
      set ssid "testvaplocalbridge"
      set local-bridging enable
      set vlanid 40 ---> only available in CLI
   next
end
```

Advertising SSIDs

- It is highly recommended to advertise the SSID. It makes it easier for customers and wireless clients. Also, if you 'hide' the SSID (known as ‘network cloaking’), then clients will always look for it when they're outside the coverage area, which searches for known SSIDs, in effect leaking the SSID anyway. Refer to RFC 3370. Furthermore, many of the latest Broadcom drivers do not support hidden SSID for WPA2.
- For security reason, you might want to prevent direct communication between your wireless clients. In this case, enable Block Intra-SSID Traffic (in the SSID configuration).
- In a network with multiple wireless controllers, you need to change the mesh SSID so that each mesh root has a unique SSID. Other controllers using the same mesh root SSID might be detected as fake or rogue APs. Go to **WiFi & Switch Controller > WiFI Network > SSID** to change the SSID. Fortinet also recommends that you create a new preshared key instead of using the default.

Using static IPs in a CAPWAP configuration

In a large FortiAP deployment with more than 20 FortiAPs connecting to a Fortigate Wireless Controller (AC), it is recommended to use static IPs on the access points instead of DHCP, setting the AC IP statically and the AC discovery type to static (Type 1), instead of learning it through broadcast, multicast, or DHCP.

This makes management of the APs easier since you know the exact IP of each access point. Troubleshooting also becomes easier as the debug of the AC controller won’t continuously attempt the different discovery methods in sequence (broadcast > multicast > static).

Logging and reporting

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled, except for traffic logging. The default logging location will be either the FortiGate unit's system memory or hard disk, depending on the model. Units with a flash disk are not recommended for disk logging.

Log management

When the FortiGate unit records FortiGate activity, valuable information is collected that provides insight into how to better protect network traffic against attacks, including misuse and abuse. There is a lot to consider before enabling logging on a FortiGate unit, such as what FortiGate activities to enable and which log device is best suited for your network's logging needs. A plan can help you in deciding the FortiGate activities to log, a log device, as well as a backup solution in the event the log device fails.

This plan should provide you with an outline, similar to the following:

- What FortiGate activities you want and/or need logged (for example, security features).
- The logging device best suited for your network structure.
- If you want or require archiving of log files.
- Ensuring logs are not lost in the event a failure occurs.

After the plan is implemented, you need to manage the logs and be prepared to expand on your log setup when the current logging requirements are outgrown. Good log management practices help you with these tasks.

Log management practices help you to improve and manage logging requirements. Logging is an ever-expanding tool that can seem to be a daunting task to manage. The following management practices will help you when issues arise, or your logging setup needs to be expanded.

- Revisit your plan on a yearly basis to verify that your logging needs are being met by your current log setup. For example, your company or organization may require archival logging, but not at the beginning of your network's lifespan. Archival logs are stored on a FortiGate unit's local hard drive, a FortiAnalyzer unit, or a FortiCloud server, in increasing order of size.
- Configure an alert message that will notify you of activities that are important to be aware about. For example: if a branch office does not have a FortiGate administrator, you will need to know at all times that the IPsec VPN tunnel is still up and running. An alert email notification message can be configured to send only if IPsec tunnel errors occur.
- If your organization or company uses peer-to-peer programs such as Skype or other instant messaging software, use the IM usage dashboard widget or the Executive Summary's report widget (Top 10 Application Bandwidth Usage Per Hour Summary) to help you monitor the usage of these types of instant messaging software. These widgets can help you in determining how these applications are being used, including if there is any misuse and abuse. Their information is taken from application log messages; however, application log messages should be viewed as well since they contain the most detailed information.
- Ensure that your backup solution is up-to-date. If you have recently expanded your log setup, you should also review your backup solution. The backup solution provides a way to ensure that all logs are not lost in the event that the log device fails or issues arise with the log device itself.

- When downloading log messages and viewing them on a computer, the log file will be downloaded like any other file. Log file names contain their log type and date in the name, so it is recommended to create a folder in which to archive your log messages, as they can be sorted easily.

System memory and hard disks

If the FortiGate unit has a hard disk, it is enabled by default to store logs. This also means that you do not have to enable this and configure the settings for logging to the hard disk, but modify these settings so that it is configured for your network logging requirements.

If the FortiGate unit has only flash memory, disk logging is disabled by default, as it is not recommended. Constant rewrites to flash drives can reduce the lifetime and efficiency of the memory. It must be enabled in the CLI under config log disk setting.

For some low-end models, disk logging is unavailable. Check a product's Feature Matrix for more information. In either case, Fortinet recommends using either a FortiAnalyzer unit or the FortiCloud service.

Chapter 6 - FortiOS Carrier

This FortiOS Handbook chapter contains the following sections:

Overview of FortiOS Carrier features provides an overview of the three major topics for FortiOS Carrier — Dynamic Profiles, MMS, and GTP.

Carrier web-based manager settings describes the web-based manager interface of FortiOS Carrier specific features.

MMS Security features describes FortiOS security features as they apply to MMS including MMS virus scanning, MMS file filtering, MMS content-based Antispam protection, and MMS DLP archiving.

Message flood protection describes setting thresholds to protect your MMS servers from receiving too many messages from the same sender.

Duplicate message protection describes setting thresholds to protect your MMS servers from receiving the same message from more than one sender.

Configuring GTP on FortiOS Carrier explains configuration of the more basic FortiOS Carrier GTP features.

GTP message type filtering explains this feature, and how to configure it on FortiOS Carrier.

GTP identity filtering explains this feature, and how to configure it on FortiOS Carrier.

Troubleshooting provides answer to common FortiOS Carrier GTP issues.

Overview of FortiOS Carrier features

FortiOS Carrier specific features include Multimedia messaging service (MMS) protection, and GPRS Tunneling Protocol (GTP) protection.

All FortiGate units, carrier-enabled or not, are capable of handling Stream Control Transmission Protocol (SCTP) traffic, which is a protocol designed for and primarily used in Carrier networks.

This section includes:

Overview
Registering FortiOS Carrier
MMS background
How FortiOS Carrier processes MMS messages
MMS protection profiles
Bypassing MMS protection profile filtering based on carrier endpoints
Applying MMS protection profiles to MMS traffic
GTP basic concepts
GPRS network common interfaces
Packet flow through the GPRS network
SCTP

Overview

FortiOS Carrier provides all the features found on FortiGate units plus added features specific to carrier networks: MMS and GTP.

MMS

MMS is a standard for sending messages that include multimedia content between mobile phones. MMS is also popular as a method of delivering news and entertainment content including videos, pictures, and text. Carrier networks include four different MMS types of messages — MM1, MM3, MM4, and MM7. See “MMS background”.

GTP

The GPRS Tunneling Protocol (GTP) runs on GPRS carrier networks. GPRS is a GSM packet radio standard. It provides more efficient usage of the radio interface so that mobile devices can share the same radio channel. FortiOS supports GTPv1 and GTPv2.

GPRS provides direct connections to the Internet (TCP/IP) and X.25 networks for point-to-point services (connection-less/connection oriented) and point-to-multipoint services (broadcast).

GPRS currently supports data rates from 9.6 kbps to more than 100 kbps, and it is best suited for burst forms of traffic. GPRS involves both radio and wired components. The mobile phone sends the message to a base station unit (radio based) that converts the message from radio to wired, and sends the message to the carrier network and eventually the Internet (wired carrier network). See GTP basic concepts.

Registering FortiOS Carrier

A license is purchased from Fortinet, and is delivered by mail as a scratch card. The contained registration code is entered into the CLI according to the instructions on the card. The FortiGate unit will then factory reset itself into Carrier mode.

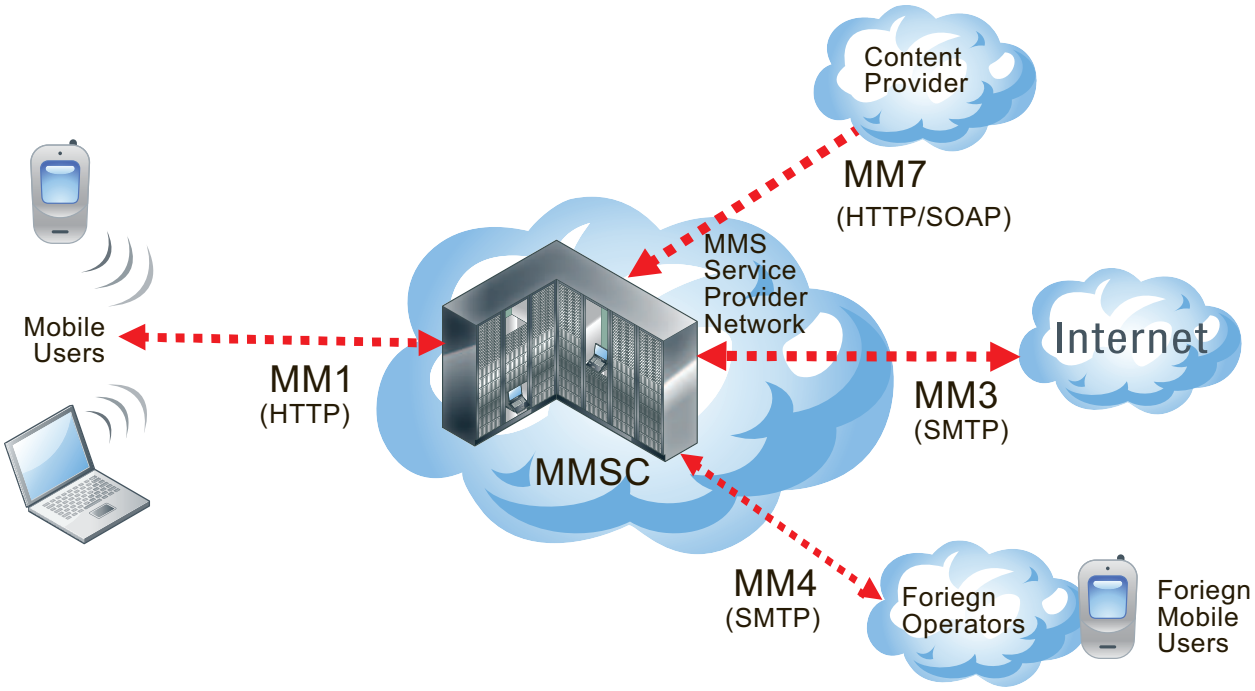
Only certain FortiGate models support Carrier mode. Contact Fortinet Support for more information and firmware images.

MMS background

MMS is a common method for mobile users to send and receive multimedia content. A Carrier network supports MMS across its network. This makes up the MMS Service Provider Network (MSPN).

Messages can be sent or received between the MMSC and a number of other services including the Internet, content providers, or other carriers. Each of these different service connections uses different MMS formats including MM1 and MM7 messages (essentially HTTP format), and MM3 and MM4 messages (SMTP formatted). These different formats reflect the different purposes and content for each type of MMS message.

MMS content interfaces



MMS content interfaces

MMS messages are sent from devices and servers to other devices and servers using MMS content interfaces

There are eight interfaces defined for the MMS standard, referred to as MM1 through MM8. The most important of these interfaces for the transfer of data is the MM1 interface, as this defines how mobile users communicate from the mobile network to the Multimedia Message Service Center (MMSC). MMS content to be monitored and controlled comes from these mobile users and is going to the provider network.

Other MMS content interfaces that connect a service provider network to other external sources can pose threats as well. MM3 handles communication between the Internet and the MMSC and is a possible source of viruses and other content problems from the Internet. MM4 handles communication between different content provider MMSCs. Filtering MM4 content protects the service provider network from content sent from foriegn service providers and their subscribers. Finally MM7 is used for communication between content providers and the MMSC. Filtering MM3 content can also keep harmful content off of the service provider network.

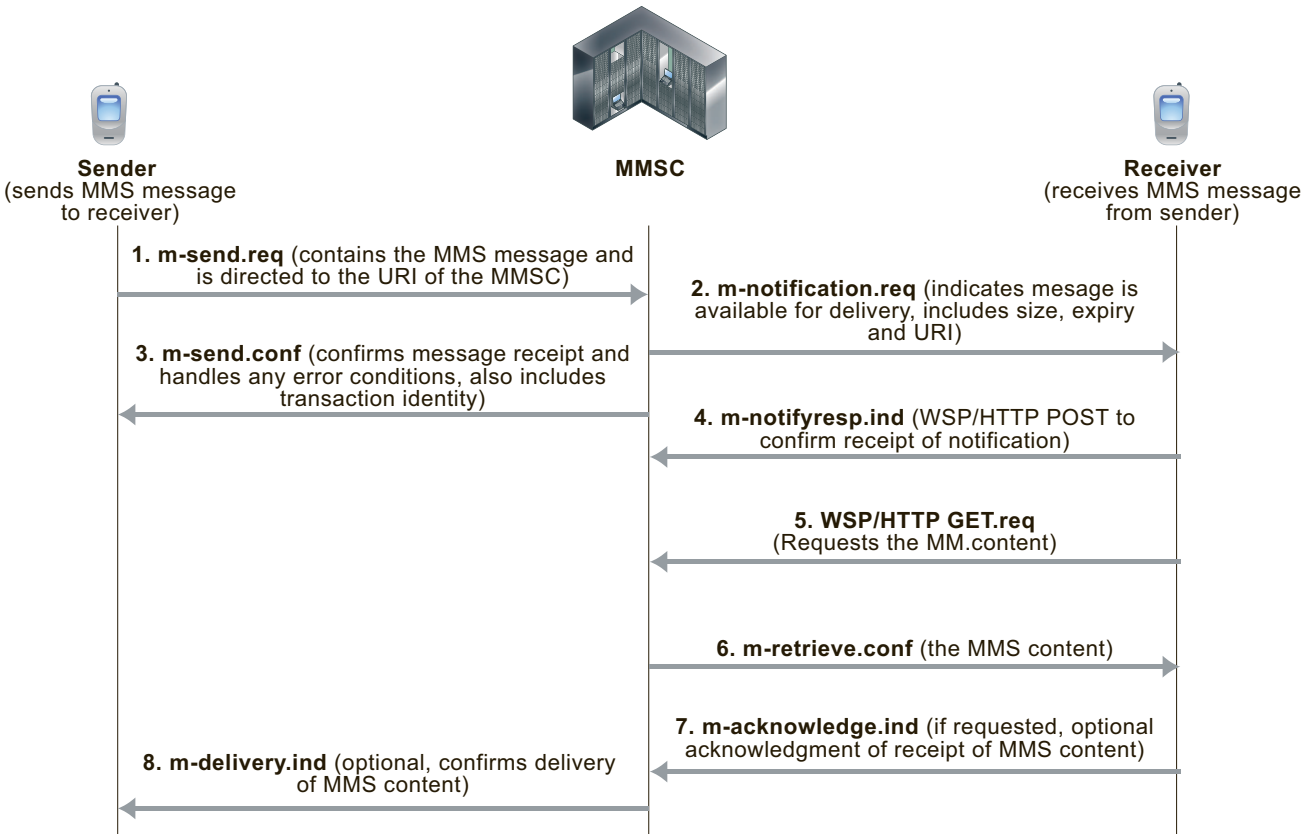
MMS content interfaces

Type	Transaction	Similar to
MM 1	Handset to MMSC	HTTP
MM 3	Between MMSC and Internet	SMTP
MM 4	Between Operator MMSCs	SMTP
MM 7	Content Providers to MMSC	HTTP and SOAP

How MMS content interfaces are applied

As shownbelow, the sender's mobile device encodes the MMS content in a form similar to MIME email message (MMS MIME content formats are defined by the MMS Message Encapsulation specification). The encoded message is then forwarded to the service provider's MMSC. Communication between the sending device and the MMSC uses the MM1 content interface. The MM1 content interface establishes a connection and sends an MM1 send request (`m-send.req`) message that contains the MMS message. The MMSC processes this request and sends back an MM1 send confirmation (`m-send.conf`) HTTP response indicating the status of the message — accepted or an error occurred, for example.

MM1 transactions between senders and receivers and the MMSC

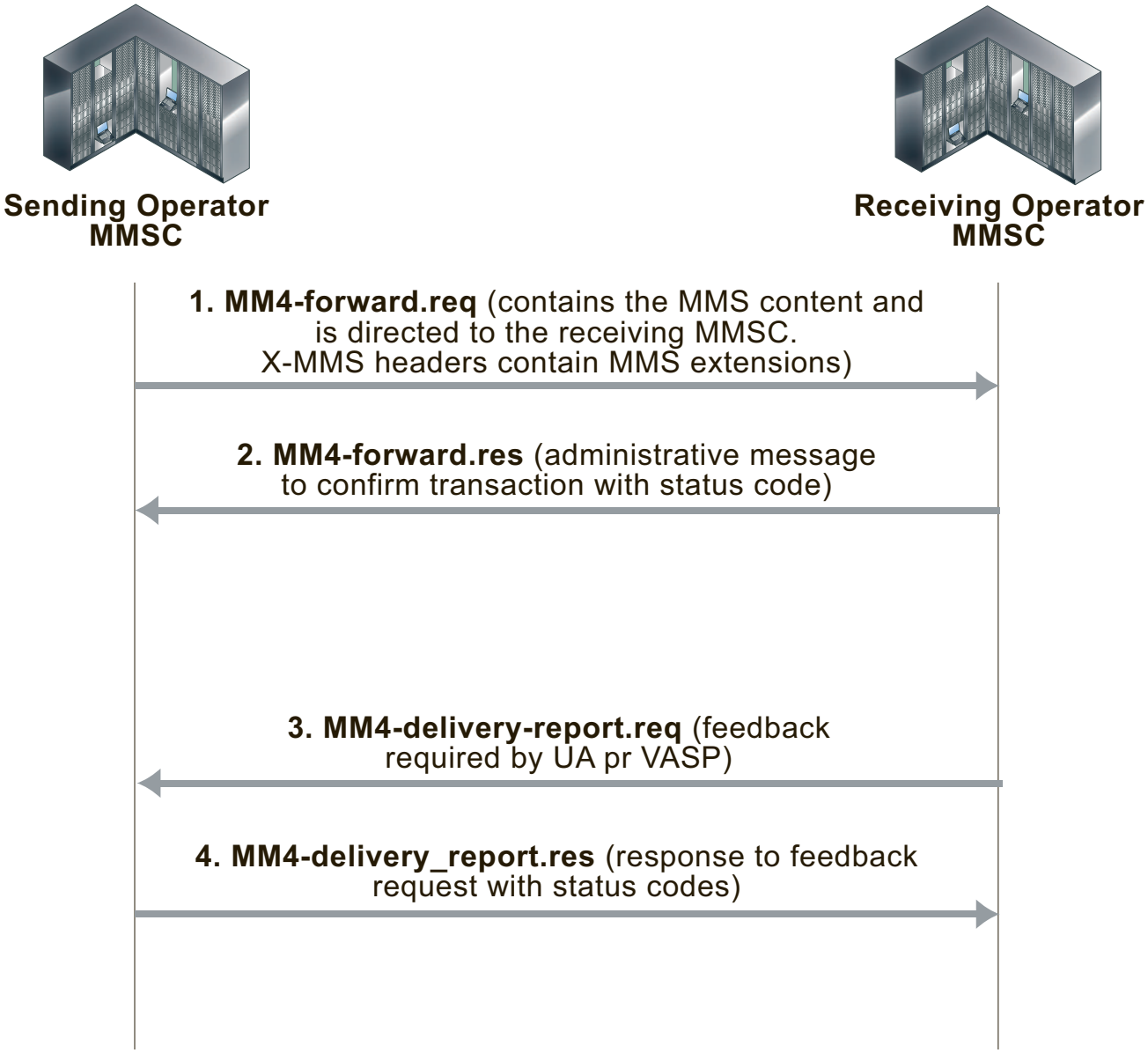


If the recipient is on another carrier, the MMSC forwards the message to the recipient's carrier. This forwarding uses the MM4 content interface for forwarding content between operator MMSCs (see the figure below).

Before the MMSC can forward the message to the final recipient, it must first determine if the receiver's handset can receive MMS messages using the MM1 content interface. If the recipient can use the MM1 content interface, the content is extracted and sent to a temporary storage server with an HTTP front-end.

To retrieve the message, the receiver's handset establishes a connection with the MMSC. An HTTP get request is then sent from the recipient to the MMSC. This message contains the URL where the content of the message is stored. The MMSC responds with a retrieve confirmation (`m-retrieve.conf`) HTTP response that contains the message.

MM4 messages sent between operator MMSCs



This causes the receiver's handset to retrieve the content from the embedded URL. Several messages are exchanged to indicate status of the delivery attempt. Before delivering content, some MMSCs also include a content adaptation service that attempts to modify the multimedia content into a format suitable for the recipient's handset.

If the receiver's handset is not MM1 capable, the message can be delivered to a web based service and the receiver can view the content from a normal Internet browser. The URL for the content can be sent to the receiver in an SMS text message. Using this method, non-MM1 capable recipients can still receive MMS content.

The method for determining whether a handset is MMS capable is not specified by the standards. A database is usually maintained by the operator, and in it each mobile phone number is marked as being associated with a

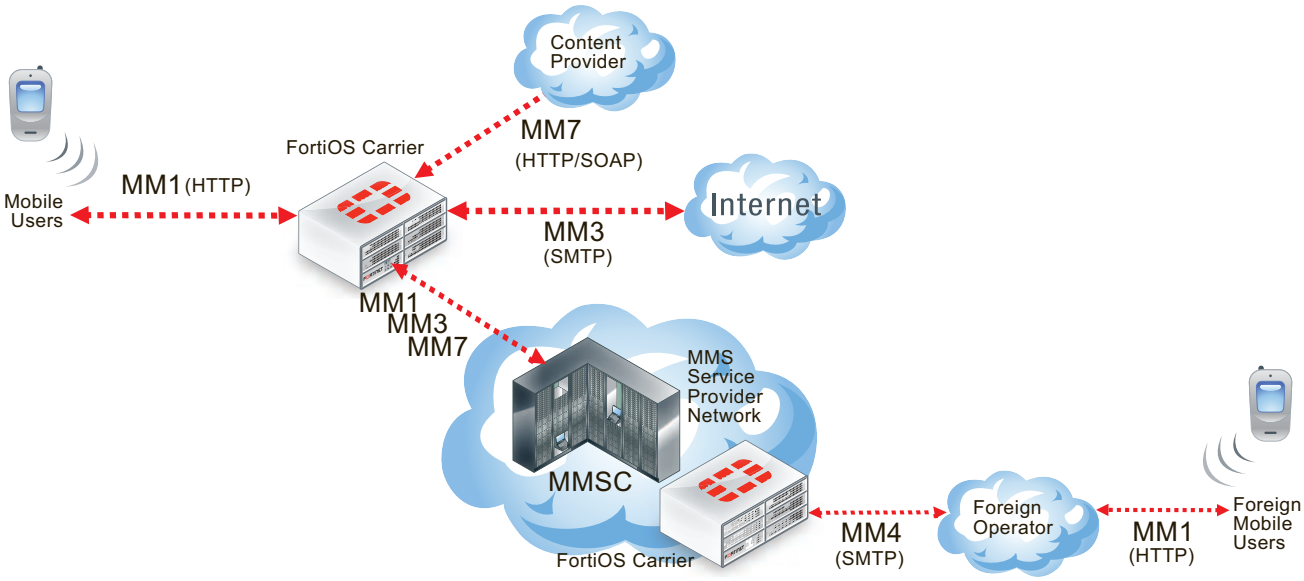
legacy handset or not. It can be a bit hit and miss since customers can change their handset at will and this database is not usually updated dynamically.

Email and web-based gateways from MMSC to the Internet use the MM3 content interface. On the receiving side, the content servers can typically receive service requests both from WAP and normal HTTP browsers, so delivery via the web is simple. For sending from external sources to handsets, most carriers allow MIME encoded message to be sent to the receiver's phone number with a special domain.

How FortiOS Carrier processes MMS messages

MMS messages can be vectors for propagating undesirable content such as spam and viruses. FortiOS Carrier can scan MMS messages sent using the MM1, MM3, MM4, and MM7 content interfaces. You can configure FortiOS Carrier to scan MMS messages for spam and viruses by configuring and adding MMS protection profiles and adding the MMS protection profiles to security policies. You can also use MMS protection profiles to apply content blocking, carrier endpoint filtering, MMS address translation, sending MMS notifications, DLP archiving of MMS messages, and logging of MMS message activity.

FortiOS Carrier MMS processing



FortiOS Carrier can send MMS messages to senders informing those senders that their devices are infected. FortiOS Carrier can also send MMS notifications to administrators to inform them of suspicious activity on their networks.

For message floods and duplicate messages, FortiOS Carrier does not send notifications to message senders but does send notifications to administrators and sends messages to sender handsets to complete MM1 and MM4 sessions.

Where MMS messaging uses the TCP/IP set of protocols, SMS text messaging uses the Signaling System Number 7 (SS7) set of protocols, which is not supported by FortiOS.

FortiOS Carrier and MMS content scanning

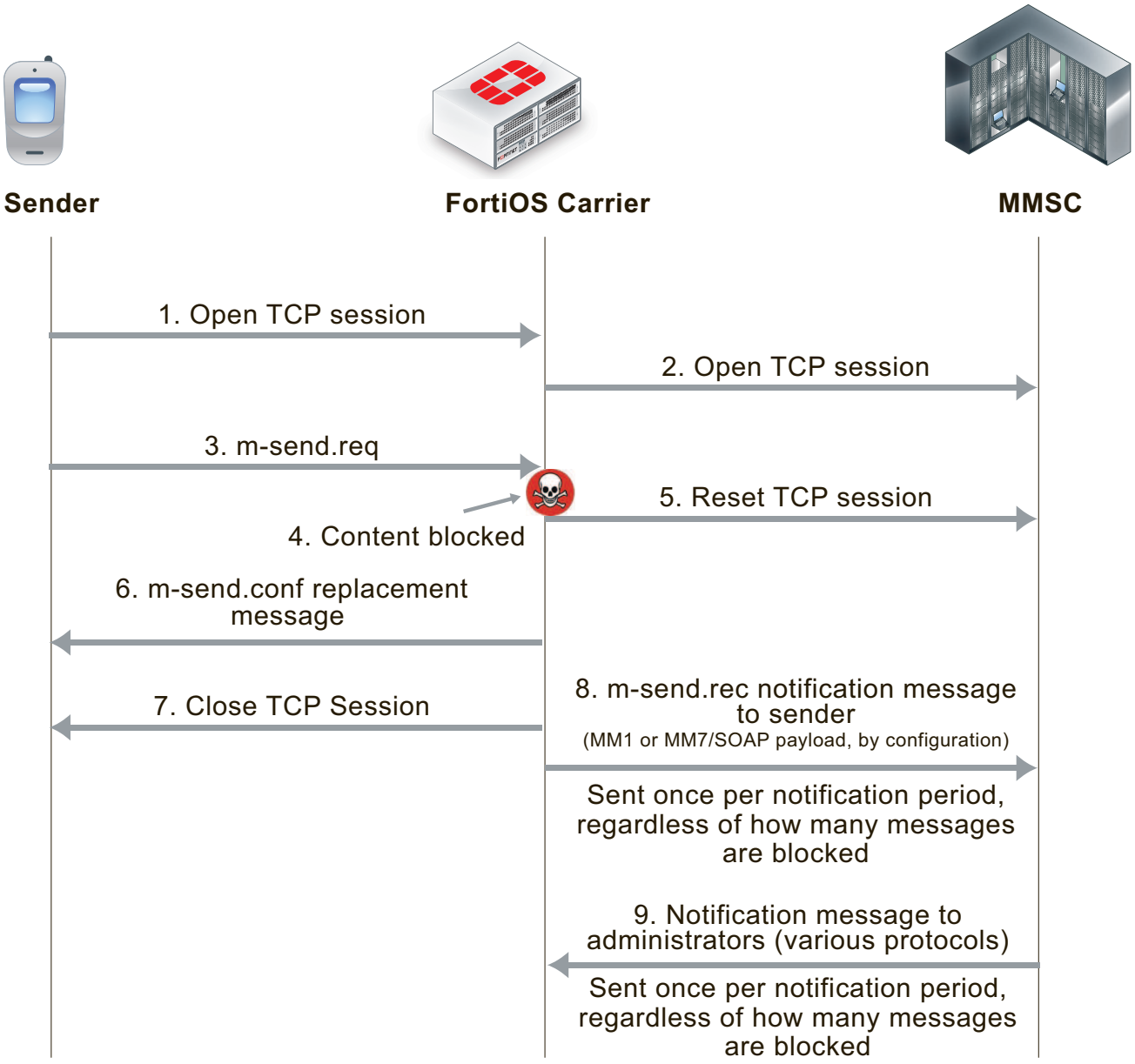
The following section applies to MMS content scanning, including virus scanning, file filtering, content spam filtering, carrier endpoint filtering, and MMS content checksum filtering.

MM1 Content Scanning

During MM1 content scanning a message is first transmitted from the sender, establishing a connection with the MMSC. FortiOS Carrier intercepts this connection and acts as the endpoint. FortiOS Carrier then establishes its own connection to the MMSC. Once connected, the client transmits its `m-send.req` HTTP post request to FortiOS Carrier which scans it according to the MMS protection profile settings. If the content is clean, the message is forwarded to the MMSC. The MMSC returns `m-send.conf` HTTP response through FortiOS Carrier to the sender.

If FortiOS Carrier blocks the message (for example because a virus was found, see the figure below), FortiOS Carrier resets the connection to the MMSC and sends `m-send.conf` HTTP response back to the sender. The response message can be customized using replacement messages. FortiOS Carrier then terminates the connection. Sending back an `m-send.conf` message prevents the sender from trying to send the message again.

MM1 MMS scanning of message sent by sender (blocking m.send.req messages)



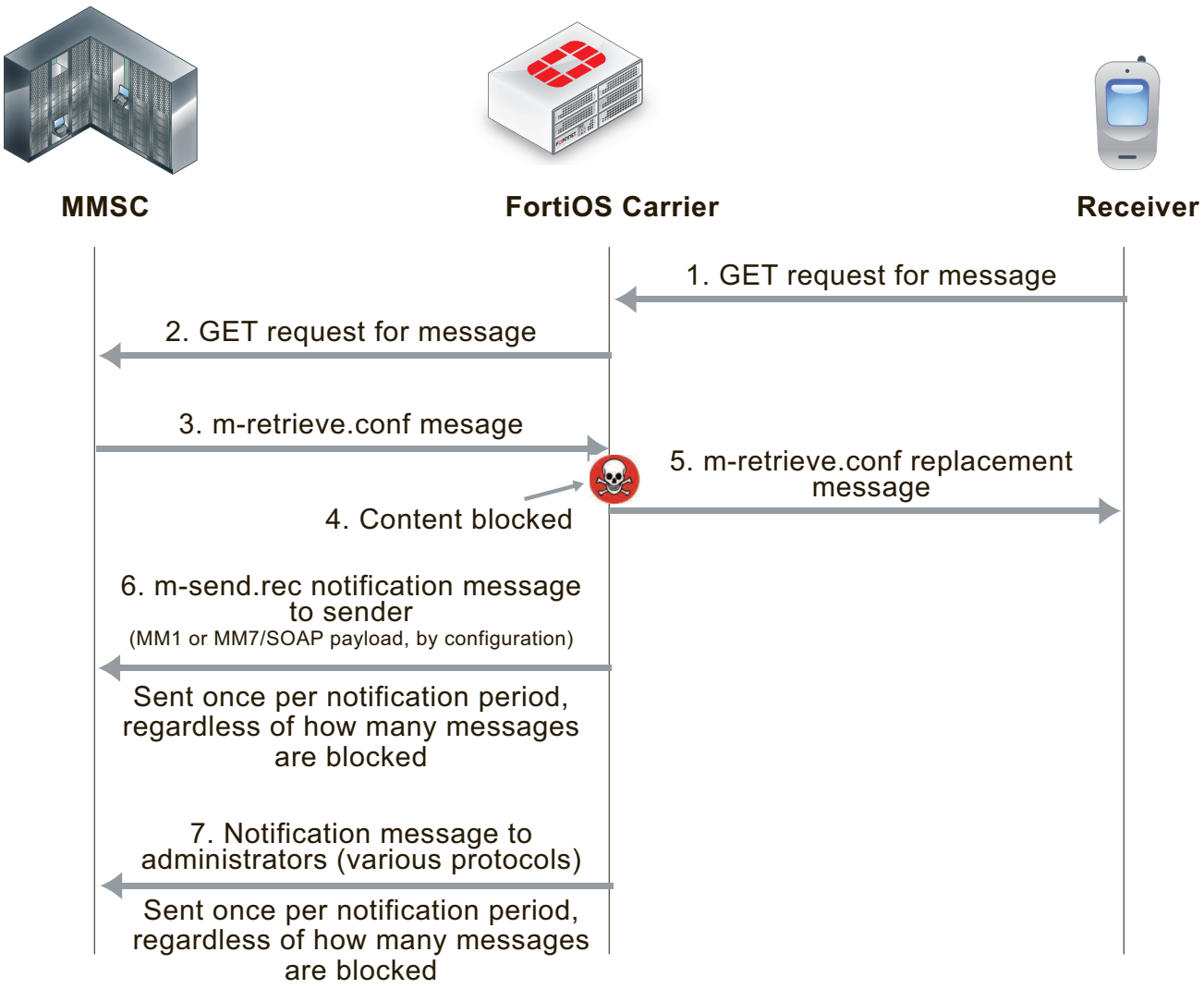
FortiOS Carrier also sends `m-send.rec` notifications messages to the MMSC that are then forwarded to the sender to notify them of blocked messages.

Filtering message retrieval

FortiOS Carrier intercepts the connection to the MMSC, and the m-retrieve.conf HTTP response from the MMSC is scanned according to the MMS content scanning settings. If the content is clean, the response is forwarded back to the client. If the content is blocked, FortiOS Carrier drops the connection to the MMSC. It then builds an m-retrieve.conf message from the associated replacement message and transmits this back to the client.

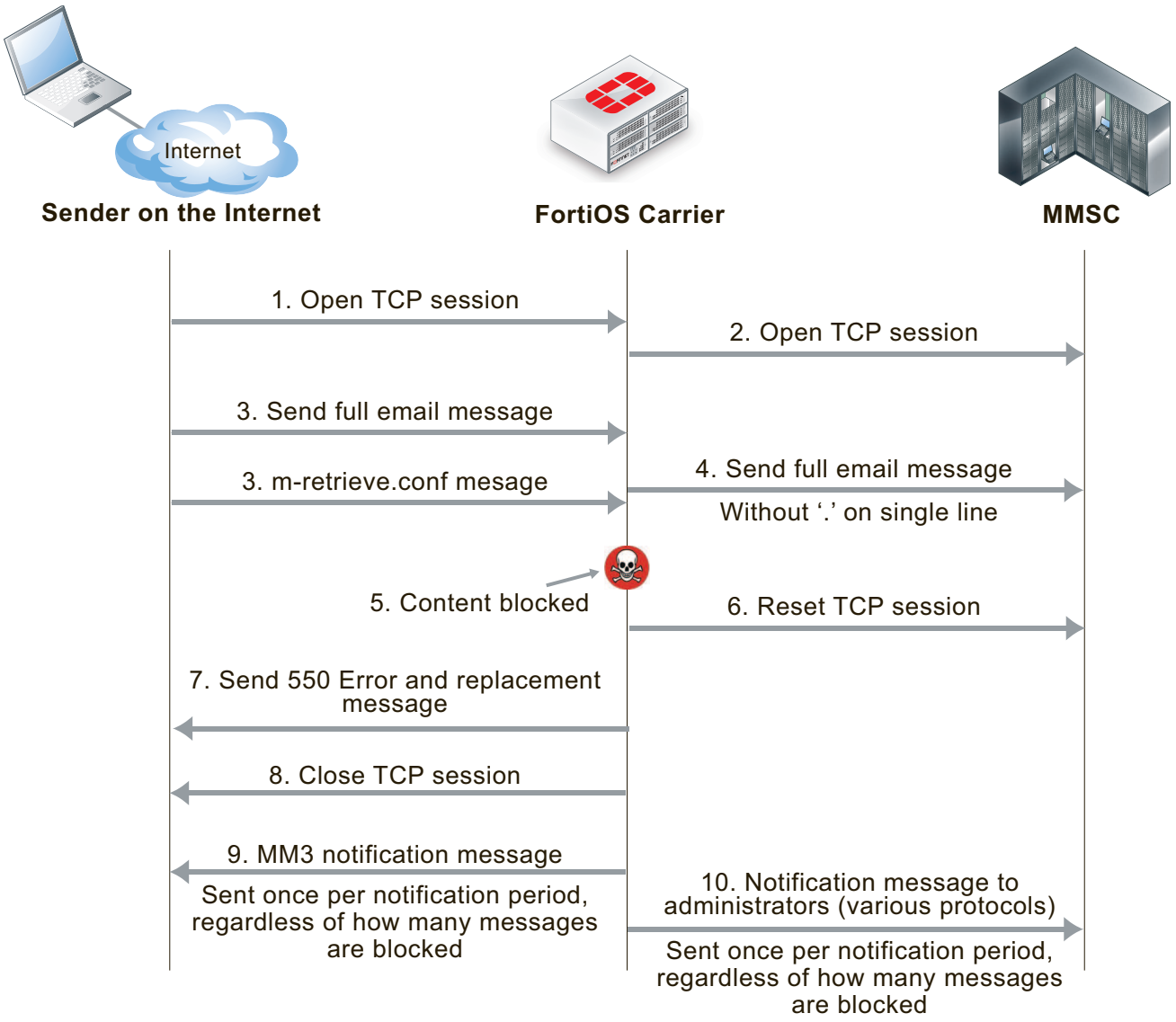
FortiOS Carrier also sends `m-send.rec` notifications messages to the MMSC that are then forwarded to the receiver to notify them of blocked messages.

MM1 MMS scanning of messages received by receiver (blocking m.retrieve.conf messages)

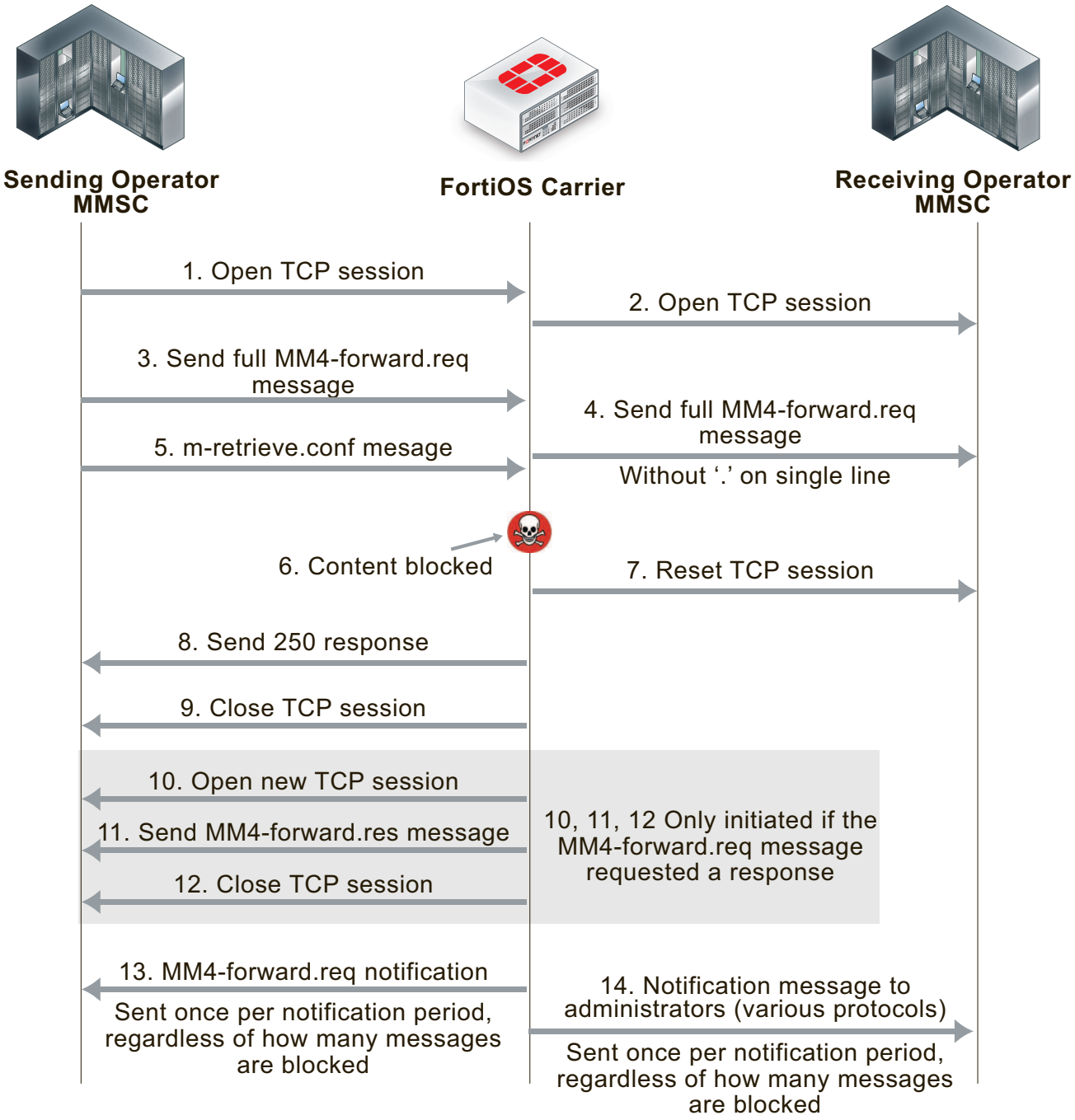


Filtering MM3 and MM4 messages works in an similar way to MM1 (see the figures below). FortiOS Carrier intercepts connections to the MMSC, and scans messages as configured. When messages are blocked, FortiOS Carrier closes sessions as required, sends confirmation messages to the sender, notifies administrators, and notifies senders and receivers of messages.

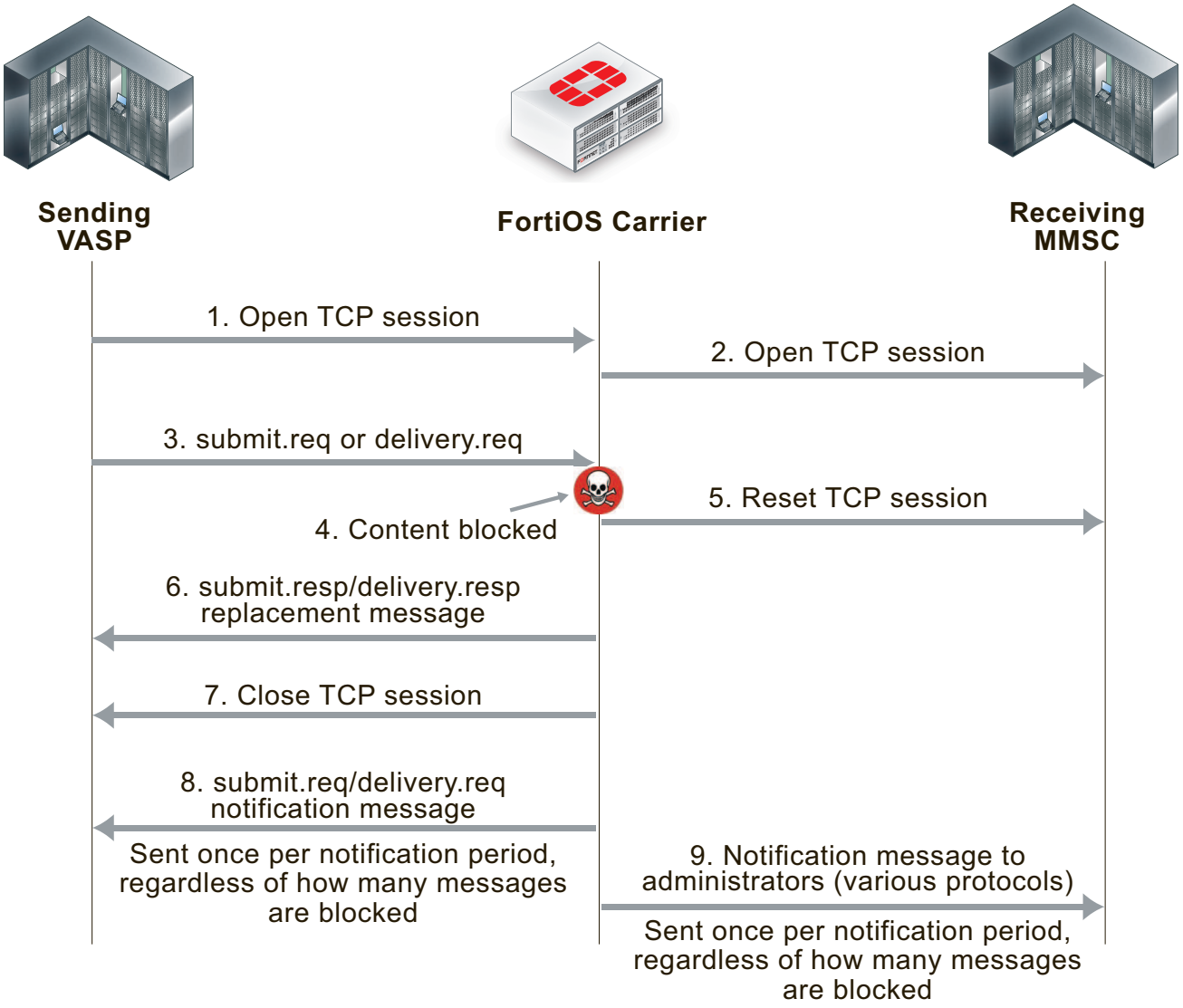
MM3 MMS scanning of messages sent from a sender on the Internet to an MMSC



MM4 MMS scanning of messages sent between operator MMSCs



MM7 MMS scanning of messages sent between a VASP and an MMSC



FortiOS Carrier and MMS duplicate messages and message floods

FortiOS Carrier detects duplicate messages and message floods for the MM1 and MM4 interfaces. How FortiOS Carrier detects and responds to duplicate messages and message floods is different from how FortiOS Carrier detects and responds to viruses and other MMS scanning protection measures.

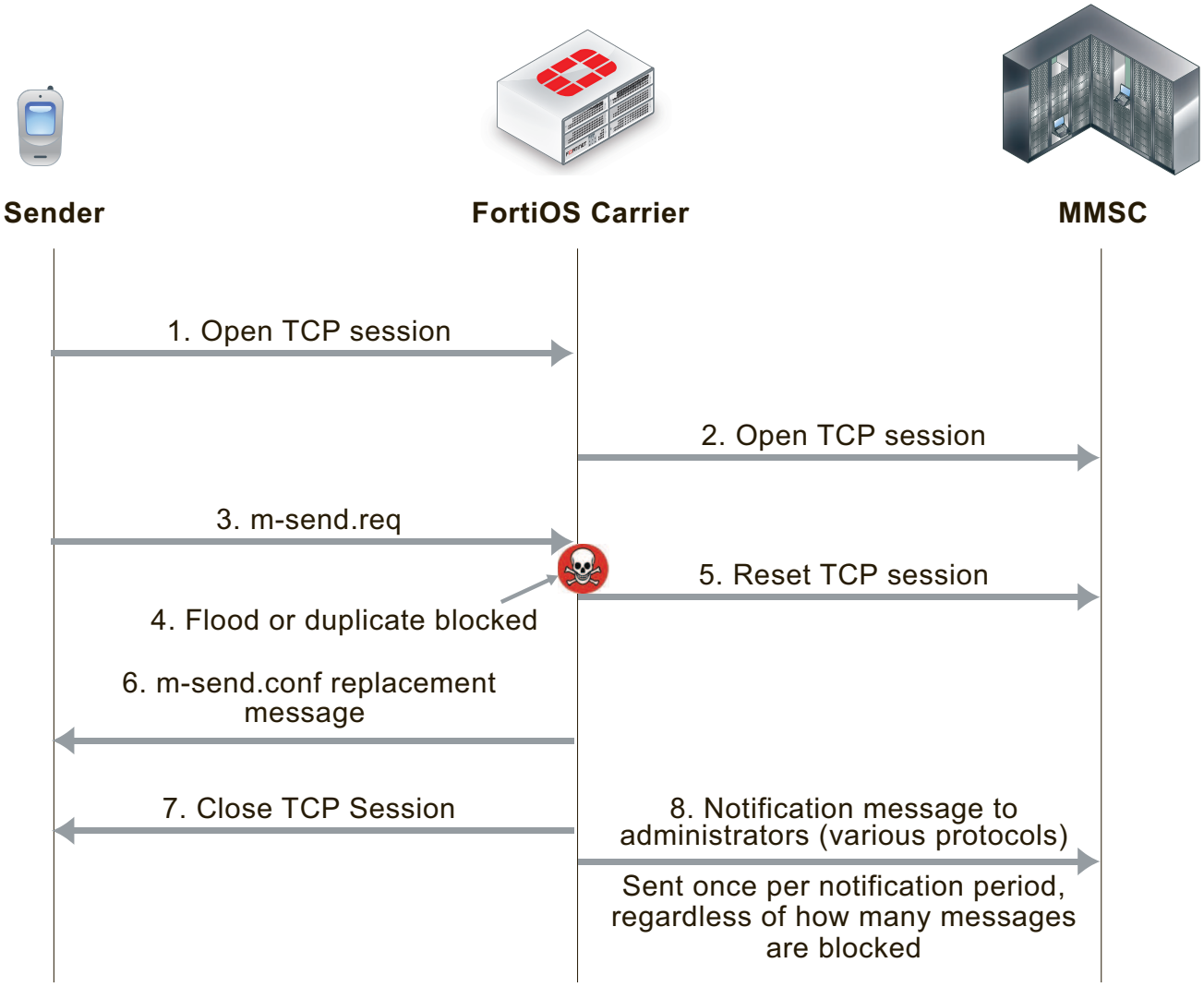
For message floods and duplicate messages, the sender does not receive notifications about floods or duplicate messages, as if the sender is an attacker they can gain useful information about flood and duplicate thresholds. Plus, duplicate messages and message floods are usually a result of a large amount of messaging activity and filtering of these messages is designed to reduce the amount of unwanted messaging traffic. Adding to the traffic by sending notifications to senders and receivers could result in an increase in message traffic.

You can create up to three thresholds for detecting duplicate messages and message floods. For each threshold you can configure the FortiOS Carrier unit to respond by logging the activity, archiving or quarantining the

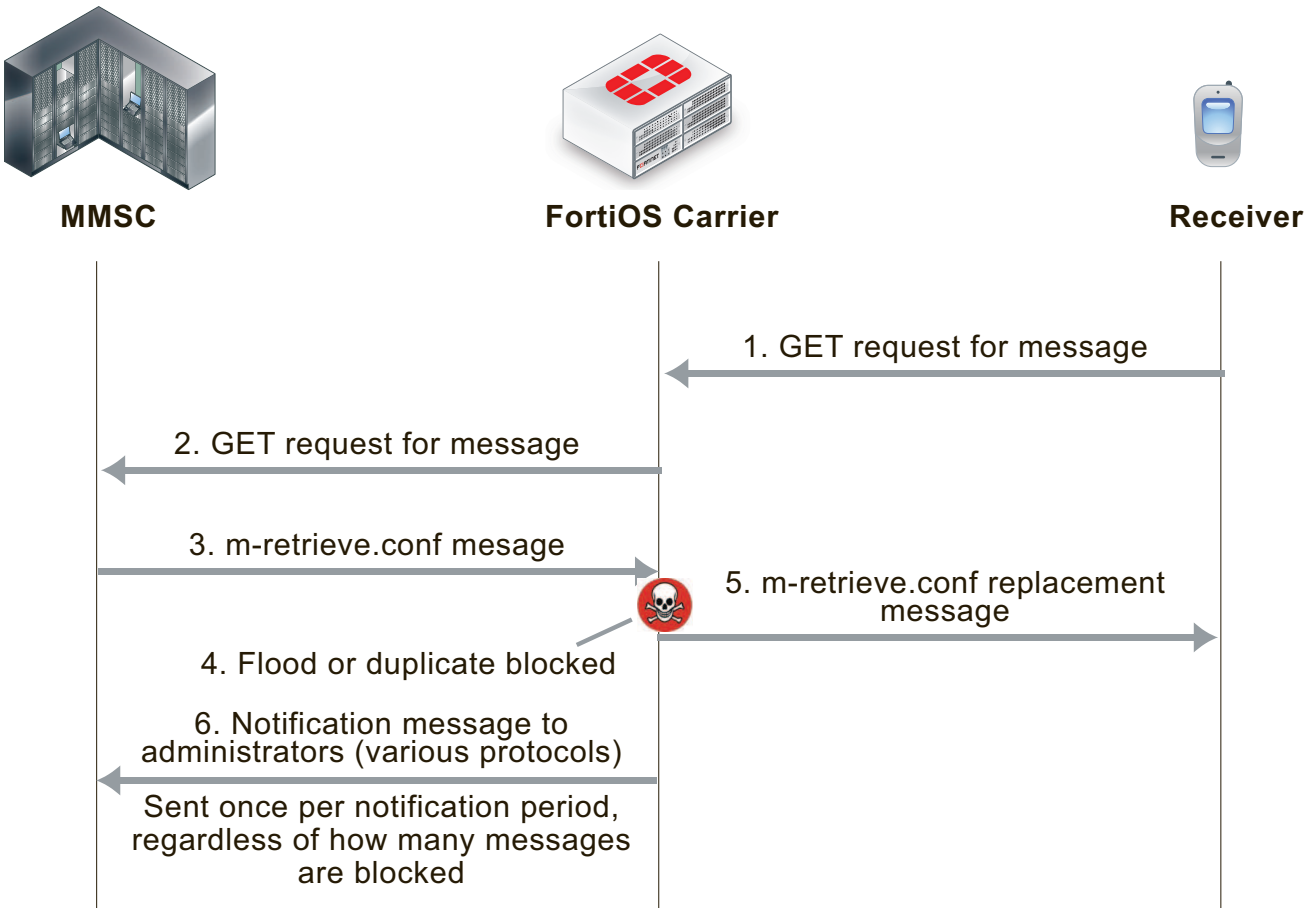
messages, notifying administrators of the activity, and by blocking the messages. In many cases you may only want to configure blocking for higher activity thresholds, and to just monitor and send administrator notifications at lower activity thresholds.

When a block threshold is reached for MM1 messages, FortiOS Carrier sends m-send.conf or m-retrieve.conf messages to the originator of the activity. These messages are sent to end the MM1 sessions, otherwise the originator would continue to re-send the blocked message. When a block threshold is reached for MM4, FortiOS Carrier sends a `MM4-forward.res` message to close the MM4 session. An MM4 message is sent only if initiated by the originating `MM4-forward.req` message.

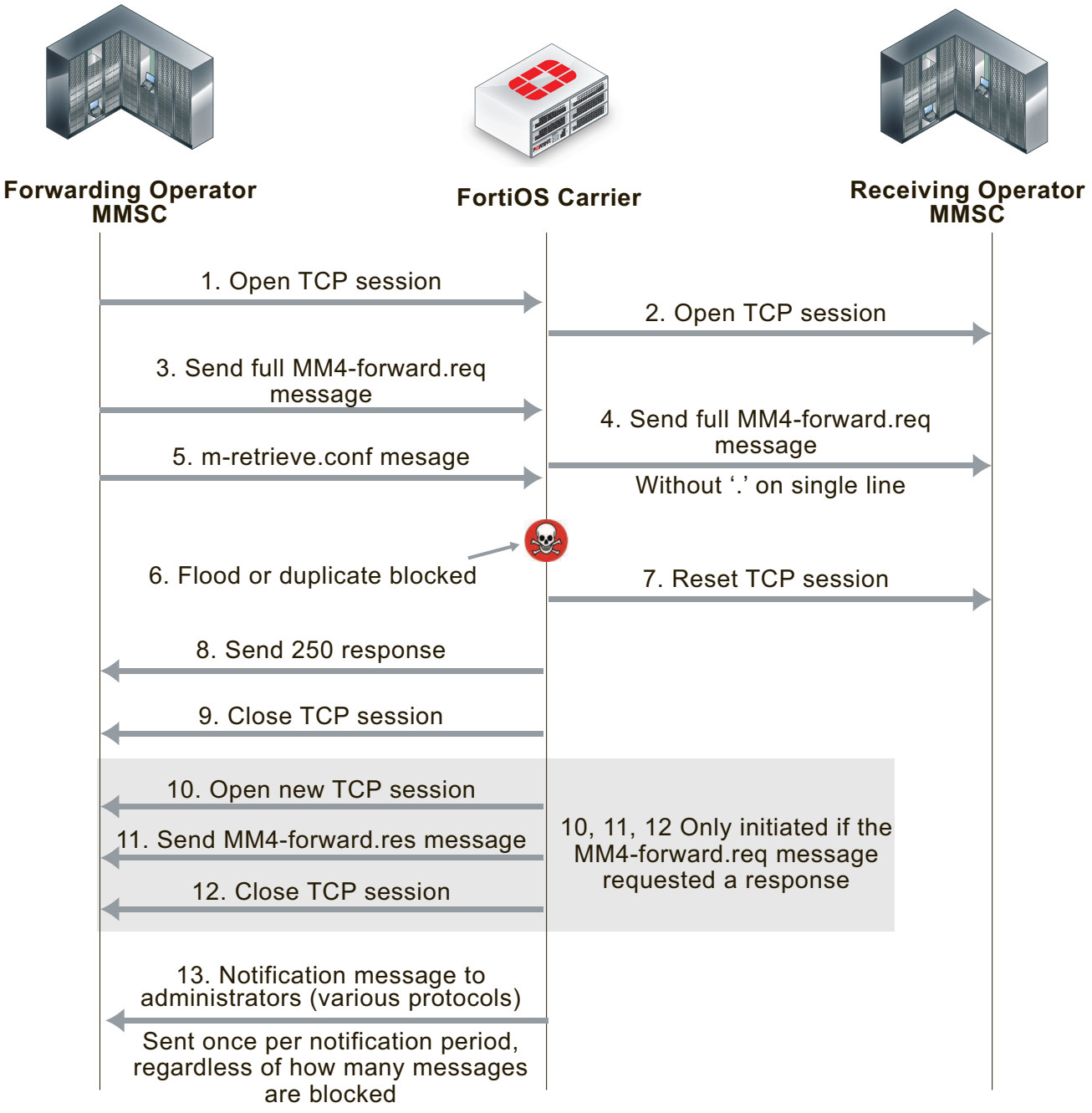
MM1 message flood and duplicate message blocking of sent messages



MM1 message flood and duplicate message blocking of received messages



MM4 message flood and duplicate message blocking



MMS protection profiles

An MMS protection profile is a group of settings that you can apply to an MMS session matched by a security policy.

MMS protection profiles are easy to configure and can be used by more than one security policy. You can configure a single MMS protection profile for the different traffic types handled by a set of security policies that

require identical protection levels and types. This eliminates the need to repeatedly configure those same MMS protection profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need only moderate protection. You would configure two separate MMS protection profiles to provide the different levels of protection: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

Once you have configured the MMS Protection Profile, you need to add it to a security policy to apply the profile to MMS traffic.

Bypassing MMS protection profile filtering based on carrier endpoints

You can use carrier endpoint filtering to exempt MMS sessions from MMS protection profile filtering. Carrier endpoint filtering matches carrier endpoints in MMS sessions with carrier endpoint patterns. If you add a carrier endpoint pattern to a filter list and set the action to exempt from all scanning, all messages from matching carrier endpoints bypass MMS protection profile filtering. See Bypassing message flood protection based on user's carrier endpoints.

Applying MMS protection profiles to MMS traffic

To apply an MMS protection profile you must first create the MMS protection profile and then add the MMS protection profile to a security policy by enabling the Carrier security profile. The MMS protection profile then applies itself to the traffic accepted by that security policy.

MMS protection profiles can contain settings relevant to many different services. Each security policy uses the subset of the MMS protection profile settings that apply to the sessions accepted by the security policy. In this way, you might define just one MMS protection profile that can be used by many security policies, each policy using a different or overlapping subset of the MMS protection profile.

To add an MMS protection profile to a security policy

1. Go to **Security Profiles > Carrier > MMS Profile**.
2. Select **Create New** to add an MMS protection profile.
3. Configure as needed, and save.
4. Go to **Policy & Objects > Policy > IPv4**.
5. Select **Create New** to add a security policy, or select an existing policy and **Edit** to add the MMS profile.
6. Configure the security policy as required.
7. Enable **MMS Profile**, and select the MMS profile to add to the security policy.
8. Select **OK**.

GTP basic concepts

GPRS currently supports data rates from 9.6kbps to more than 100 kbps, and is best suited for burst forms of traffic. GPRS involves both radio and wired components. The mobile phone sends the message to a base station unit (radio based), and the base station unit sends the message to the carrier network and eventually the Internet (wired carrier network).

The network system then either sends the message back to a base station and to the destination mobile unit, or forwards the message to the proper carrier's network where it gets routed to the mobile unit.

PDP Context

The packet data protocol (PDP) context is a connection between a mobile station and the end address that goes through the SGSN and GGSN. It includes identifying information about the mobile customer used by each server or device to properly forward the call data to the next hop in the carrier network, typically using a GTP tunnel between the SGSN and GGSN.

When a mobile customer has an active voice or data connection open, both the SGSN and GGSN have the PDP context information for that customer and session.

When a mobile phone attempts to communicate with an address on an external packet network, either an IP or X.25 address, the mobile station that phone is connected to opens a PDP context through the SGSN and GGSN to the end address. Before any traffic is sent, the PDP context must first be activated.

The information included in the PDP context includes the customer's IP address, the IMSI number of the mobile handset, and the tunnel endpoint ID for both the SGSN and GGSN. The ID is a unique number, much like a session ID on a TCP/IP firewall. All this information ensures a uniquely identifiable connection is made.

Since one mobile device may have multiple connections open at one time, such as data connections to different Internet services and voice connections to different locations, there may be more than one PDP context with the same IP address making the extra identifying information required.

The endpoint that the mobile phone is connecting to only knows about the GGSN — the rest of the GPRS connection is masked by the GGSN.

Along the PDP context path, communication is accomplished in using three different protocols.

- The connection between the Mobile Station and SGSN uses the SM protocol.
- Between SGSN and GGSN GTP is used.
- Between GGSN and the endpoint either IP or X.25 is used.

FortiOS Carrier is concerned with the SGSN to GGSN part of the PDP context — the part that uses GTP.

For more about PDP context, see Tunnel Management Messages.

Creating a PDP context

While FortiOS Carrier is concerned mostly with the SGSN to GGSN part of the PDP Context, knowing the steps involved in creating a PDP context helps understand the role each device, protocol, and message type plays.

Both mobile stations and GGSNs can create PDP contexts.

A Mobile Station creates a PDP context

1. The Mobile Station (MS) sends a `PDP activation request` message to the SGSN including the MS PDP address, and APN.
2. Optionally, security functions may be performed to authenticate the MS.
3. The SGSN determines the GGSN address by using the APN identifier.
4. The SGSN creates a downlink GTP tunnel to send IP packets between the GGSN and SGSN.
5. The GGSN creates an entry in its PDP context table to deliver IP packets between the SGSN and the external packet switching network.
6. The GGSN creates an uplink GTP tunnel to route IP-PDU from SGSN to GGSN.

7. The GGSN then sends back to the SGSN the result of the PDP context creation and if necessary the MS PDP address.
8. The SGSN sends an `Activate PDP context accept` message to the MS by returning negotiated the PDP context information and if necessary the MS PDP address.
9. Now traffic can pass from the MS to the external network endpoint.

A GGSN creates a PDP context

1. The network receives an IP packet from an external network.
2. The GGSN checks if the PDP Context has already been created.
3. If not, the GGSN sends a `PDU notification request` to the SGSN in order to initiate a PDP context activation.
4. The GGSN retrieves the IP address of the appropriate SGSN address by interrogating the HLR from the IMSI identifier of the MS.
5. The SGSN sends to the MS a request to activate the indicated PDP context.
6. The PDP context activation procedure follows the one initiated by the MS. See "A Mobile Station creates a PDP context".
7. When the PDP context is activated, the IP packet can be sent from the GGSN to the MS.

Terminating a PDP context

A PDP context remains open until it is terminated. To terminate the PDP context an MS sends a `Deactivate PDP context` message to the SGSN, which then sends a `Delete PDP Context` message to the GGSN. When the SGSN receives a PDP context deletion acknowledgment from the GGSN, the SGSN confirms to the MS the PDP context deactivation. The PDP can be terminated by the SGSN or GGSN as well with a slight variation of the order of the messages passed.

When the PDP Context is terminated, the tunnel it was using is deleted as well. If this is not completed in a timely manner, it is possible for someone else to start using the tunnel before it is deleted. This hijacking will result in the original customer being overbilled for the extra usage. Anti-overbilling helps prevent this. See Configuring Anti-overbilling in FortiOS Carrier.

GPRS security

The GPRS network has some built-in security in the form of GPRS authentication. However this is minimal, and is not sufficient for carrier network security needs. A GTP firewall, such as FortiOS Carrier, is required to secure the Gi, Gn, and Gp interfaces.

GPRS authentication

GPRS authentication is handled by the SGSN to prevent unauthorized GPRS calls from reaching the GSM network beyond the SGSN (the base station system, and mobile station). Authentication is accomplished using some of the customer's information with a random number and uses two algorithms to create ciphers that then allow authentication for that customer.

User identity confidentiality ensures that customer information stays between the mobile station and the SGSN — no identifying information goes past the SGSN. Past that point other numbers are used to identify the customer and their connection on the network.

Periodically the SGSN may request identity information from the mobile station to compare to what is on record, using the IMEI number.

Call confidentiality is achieved through the use of a cipher, similar to the GPRS authentication described earlier. The cipher is applied between the mobile station and the SGSN. Essentially a cipher mask is XORd with each outgoing frame, and the receiving side XORs with its own cipher to result in the original frame and data.

Parts of a GTPv1 network

A sample GTP network consists of the end handset sender, the sender's mobile station, the carrier's network including the SGSN and GGSN, the receiver's mobile station, and the receiver handset.

When a handset moves from one mobile station and SGSN to another, the handset's connection to the Internet is preserved because the tunnel the handset has to the Internet using GTP tracks the user's location and information. For example, the handset could move from one cell to another, or between countries.

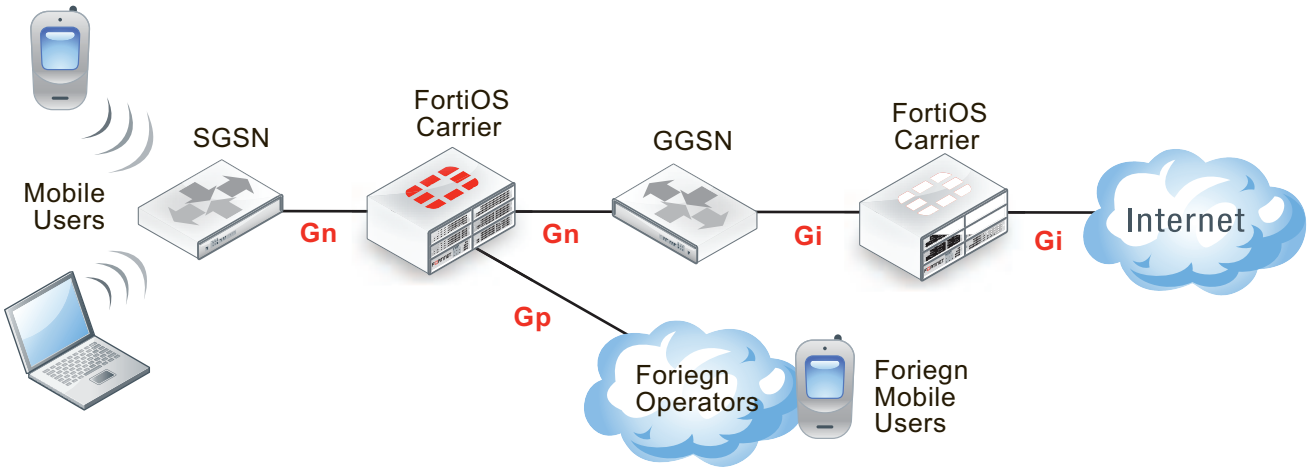
The parts of a GPRS network can be separated into the following groups according to the roles of the devices:

- Radio access to the GPRS network is accomplished by mobile phones and mobile stations (MS).
- Transport the GPRS packets across the GPRS network is accomplished by SGSNs and GGSNs, both local and remote, by delivering packets to the external services.
- Billing and records are handled by CDF, CFR, HLR, and VLR devices.

GPRS networks also rely on access points and PDP contexts as central parts of the communication structure. These are not actual devices, but they are still critical .

These devices, their roles, neighboring devices, the interfaces and protocols they use are outlined in the following table.

Carrier network showing the interfaces used (GTPv1)



Devices on a GTPv1 network

Device role	Neighboring Devices	Interfaces used	Protocols used
Mobile Users	Mobile Stations (MS)	Radio Access Technology (RAT)	
Mobile Stations (MS)	Mobile Users, SGSN	Gb	IP, Frame Relay
SGSN (local)	MS, SGSN (local or remote), GGSN (local and remote), CDR, CFR, HLR, VLR	Ga, Gb, Gn, Gp, Gz	IP, Frame Relay, GTP, GTP'
SGSN (remote)	SGSN (local)	Gn	GTP
GGSN (local)	SGSN (local or remote), GGSN (local and remote), CDR, CFR, HLR, VLR	Ga, Gi, Gn, Gp, Gz	IP, GTP, GTP'
GGSN (remote)	SGSN (local), WAP gateway, Internet, other external services	Gi, Gp	IP, GTPv1
CDR, CFR	SGSN (local), GGSN (local)	Ga, Gz	GTP'
HLR, VLR	SGSN (local), GGSN (local)	Ga, Gz	GTP'

Radio access

For a mobile phone to access the GPRS core network, it must first connect to a mobile station. This is a cellular tower that is connected to the carrier network.

How the mobile phone connects to the mobile station (MS) is determined by what Radio Access Technologies (RATs) are supported by the MS.

Transport

Transport protocols move data along the carrier network between radio access and the Internet or other carrier networks.

FortiOS Carrier should be present where information enters the Carrier network, to ensure the information entering is correct and not malicious. This means a Carrier-enabled FortiGate unit intercepts the data coming from the SGSN or foreign networks destined for the SSGN or GGSN onto the network, and after the GGSN as the data is leaving the network.

GTP

GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry General Packet Radio Service (GPRS) within Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. It allows carriers to transport actual cellular packets over their

network via tunneling. This tunneling allows users to move between SGSNs and still maintain connection to the the Internet through the GGSN.

GTP has three versions version 0, 1, and 2. GTP1 and GTP2 are supported by FortiOS Carrier. The only GTP commands that are common to all forms of GTP are the echo request/response commands that allow GSNs to verify up to once every 60 seconds that neighboring GSNs are alive.

GTPv0

There have been three versions of GTP to date. The original version of GTP (version 0) has the following differences from version GTPv1.

- the tunnel identification is not random
- there are options for transporting X.25
- the fixed port number 3386 is used for all functions, not just charging
- optionally TCP is allowed as a transport instead of UDP
- not all message types are supported in version 0

GTPv1

On a GPRS network, Packet Data Protocol (PDP) context is a data structure used by both the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The PDP context contains the subscribers information including their access point, IP address, IMSI number, and their tunnel endpoint ID for each of the SGSN and GGSN.

The Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address(es) used in the packet data network) of all GPRS users registered with this SGSN.

GTPv1-C

GTPv1-C refers to the control layer of the GPRS Transmission network. This part of the protocol deals with network related traffic.

FortiOS Carrier handles GTPv1-C in GTPv1 by using the Tunnel Endpoint IDentifier (TEID), IP address and a Network layer Service Access Point Identifier (NSAPI), sometimes called the application identifier, as an integer value that is part of the PDP context header information used to identify a unique PDP context in a mobile station, and SGSN.

For more information on GTPv1-C, see GTP-C messages.

GTPv1-U

GTPv1-U is defined in 3GPP TS 29.281 and refers to the user layer of the GPRS Tunneling network. This part of the protocol deals with user related traffic, user tunnels, and user administration issues.

A GTPv1-U tunnel is identified by a TEID, an IP address, and a UDP port number. This information uniquely identifies the limb of a GTPv1 PDP context. The IP address and the UDP port number define a UDP/IP path, a connectionless path between two endpoints (i.e. SGSN or GGSN). The TEID identifies the tunnel endpoint in the

receiving GTPv1-U protocol entity; it allows for the multiplexing and demultiplexing of GTP tunnels on a UDP/IP path between a given GSN-GSN pair. For more information on GTPv1-U, see GTP-U messages.

The GTP core network consists of one or more SGSNs and GGSNs.

GGSN

The Gateway GPRS Support Node (GGSN) connects the GPRS network on one side via the SGSN to outside networks such as the Internet. These outside networks are called packet data networks (PDNs). The GGSN acts as an edge router between the two different networks — the GGSN forwards incoming packets from the external PDN to the addressed SGSN and the GGSN also forwards outgoing packets to the external PDN. the GGSN also converts the packets from the GPRS packets with SGSN to the external packets, such as IP or X.25.

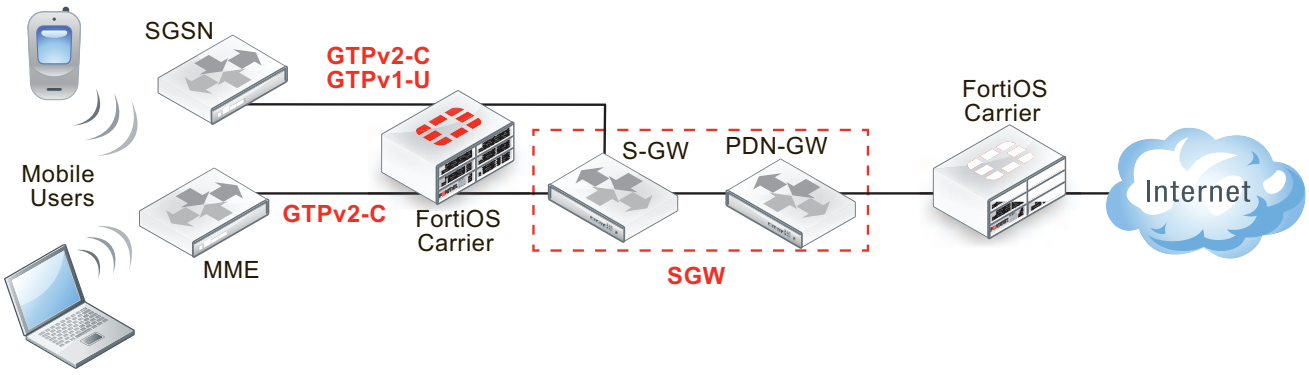
SGSN

The Serving GPRS Support Node (SGSN) connects the GPRS network to GTPv1 compatible mobile stations, and mobile units (such as UTRAN and ETRAN) on one side and to the gateway node (GGSN), which leads to external networks, on the other side. Each SGSN has a geographical area, and mobile phones in that area connect to the GPRS network through this SGSN. The SGSN also maintains a location register that contains customer's location and user profiles until they connect through a different SGSN at which time the customer information is moved to the new SGSN. This information is used for packet routing and transfer, mobility management also known as location management, logical link management, and authentication and billing functions.

GTPv2

GTPv2, defined in 3GPP TS 29.274, is dramatically differnet from GTPv1, defined in 3GPP TS 29.060. Where in GTPv1 the tunnel is between the SGSN and the GGSN, in GTPv2 The SGSN is between the MME and the LTE Serving Gateway (S-GW), beyond which is the PDN gateway (P-GW). Even tunnel management messages have changed significantly.

Network diagram for GTPv2



Device roles on a GTPv2 network

Device role	Neighboring Devices	Interfaces used	Protocols used
Mobile Users	Mobile Stations (MS)	Radio Access Technology (RAT)	--
GTPv1 Mobile Stations (MS)	Mobile Users, SGSN	Gb	IP, Frame Relay
GTPv2 Mobile Stations (MS)	Mobile Users, MME	???	IP, Frame Relay
SGSN (local)	GTPv1 MS, SGSN, S-GW	???	IP, Frame Relay, GTPv1, GTP'
S-GW	SGSN, MME, P-GW	???	IP, GTPv2, GTP'
P-GW	S-GW, Internet, other external services	???	IP, GTPv2

GTPv2-C

GTPv2-C is the control layer messaging for GTPv2. It is used by LTE mobile stations, SGSN units for backwards compatibility, and SGWs that are the gateway to other networks. The messaging is very different from GTPv1. GTPv2-C is required to communicate with the Mobility Management Entity (MME) to create, change and delete EPS bearers when handover events happen, and to create Forwarding tunnels. The protocol is also used to communicate with the Serving Gateway (SGW) which has the S-GW and PDN-GW interfaces, and the Serving GPRS Support Node (SGSN).

MME

MME essentially fills the role of the SGSN in a GTPv1 network — it is how the mobile stations gain access to the Carrier network. GTPv2 supports different mobile stations than GTPv1, so MME handles the GTPv2 MSes and SGSN handles the GTPv1 MSes

Billing and records

A major part of the GPRS network is devoted to billing. Customer billing requires enough information to identify the customer, and then billing specific information such as connection locations and times, as well as amount of data transferred. A modified form of GTP called GTP' is used for billing. The home location records and visitor location records store information about customers that is critical to billing.

GTP' (GTP prime)

GTP is used to handle tunnels of user traffic between SGSNs and GGSNs. However for billing purposes, other devices that are not supported by GTP are required. GTP' (GTP prime) is a modified form of GTP and is used to communicate with these devices such as the Charging Data Function (CDF) that communicates billing information to the Charging Gateway Function (CGF). In most cases, GTP' transports user records from many individual network elements, such as the GGSNs, to a centralised computer which then delivers the charging data

more conveniently to the network operator's billing center, often through the CGF. The core network sends charging information to the CGF, typically including PDP context activation times and the quantity of data which the end user has transferred.

GTP' is used by the Ga and Gz interfaces to transfer billing information. GTP' uses registered UDP/TCP port 3386. GTP' defines a different header, additional messages, field values, as well as a synchronisation protocol to avoid losing or duplicating CDRs on CGF or SGSN/GGSN failure. Transferred CDRs are encoded in ASN.1.

HLR

The Home Location Register (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time. The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

VLR

The Visitor Location Register (VLR) is a database which stores information about all the mobile devices that are currently under the jurisdiction of the Mobile Switching Center which it serves. Of all the information the VLR stores about each Mobile Station, the most important is the current Location Area Identity (LAI). This information is vital in the call setup process.

Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it also updates the HLR of the mobile subscriber, informing it of the new location of that MS.

For more information on GTP', see GTP-U and Charging Management Messages.

GPRS network common interfaces

There are interfaces for each connection on the GPRS network. An interface is an established standard form of communication between two devices. Consider a TCP/IP network. In addition to the transport protocol (TCP) there are other protocols on that network that describe how devices can expect communications to be organized, just like GPRS interfaces.

Interfaces between devices on the network

There are a series of interfaces that define how different devices on the carrier network communicate with each other. There interfaces are called Ga to Gz, and each one defines how a specific pair of devices will communicate. For example Gb is the interface between the base station and the SGSN, and Gn is one possible interface between the SGSN and GGSN.

The SGSN and GGSN keep track of the CDR information and forward it to the Charging Data Function (CDF) using the Gr interface between the SGSN and home location register (HLR), Gs interface between the SGSN and MSC (VLR), Gx interface between the GGSN and the Charging Rules Function (CRF), Gy between the GGSN and online charging system (OCS), and finally Gz which is the off-line (CDR-based) charging interface between the GSN and the CG that uses GTP'.

Each of these interfaces on the GPRS network is has a name in the format of `Gx` where `x` is a letter of the alphabet that determines what part of the network the interface is used in. It is common for network diagrams of GPRS networks to include the interface name on connections between devices.

The Carrier-enabled FortiGate unit only provides protection on the Gn, Gp, and Gi interfaces.

GPRS network interfaces, their roles, and billing

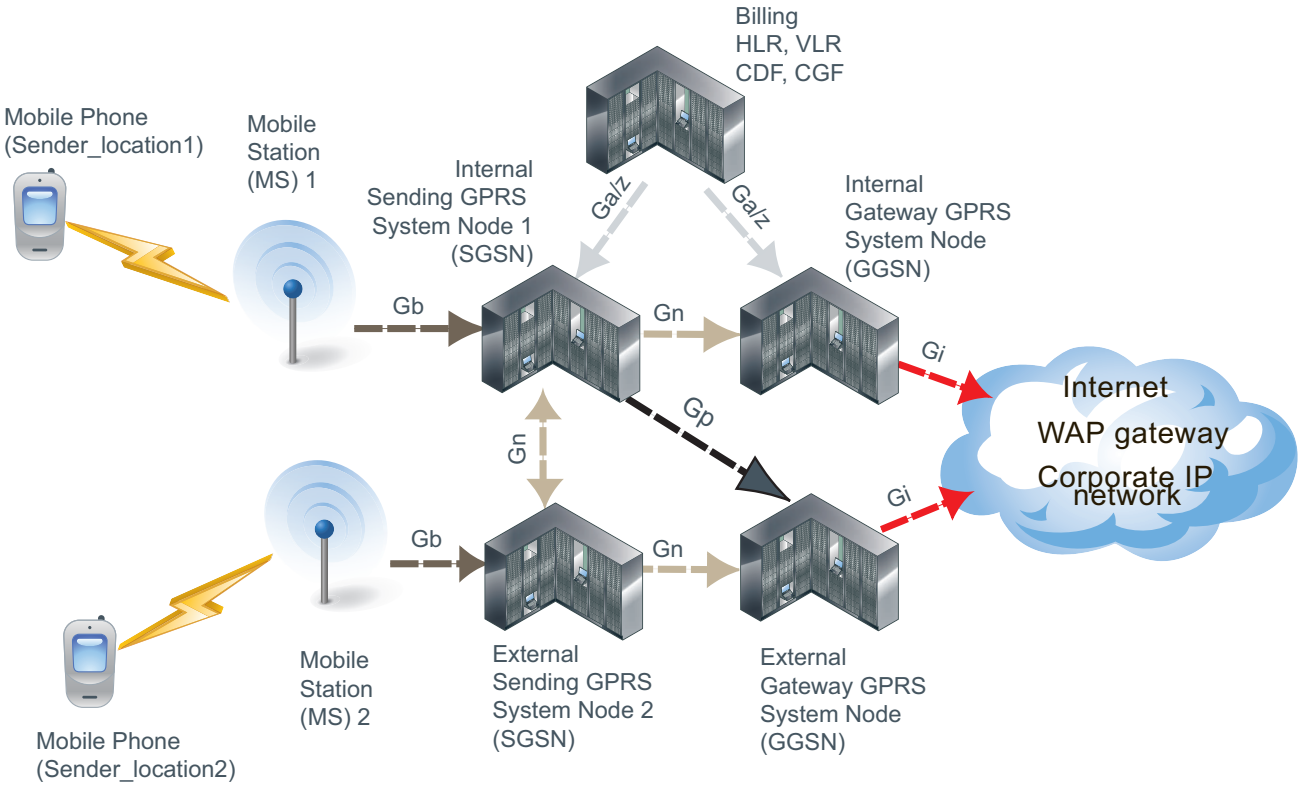
Name	Device connections that use this interface	Traffic Protocol used	Its role or how it affects billing
Ga	CDR and GSN (SGSNs and GGSNs)	GTP' - GTP modified to include CDR role	CDR have the accounting records, that are compiled in the GSN and then sent to the Charging Gateway (CG)
Gb	MS and SGSN	Frame Relay or IP	When an IP address moves to a new MS, the old MS may continue to use and bill that IP address.
Gi	GGSN and public data networks (PDNs)	IP based	This is the connection to the Internet. If the GTP tunnel is deleted without notifying the Gi interface, the connection may remain open incurring additional charges. FortiOS Carrier adds this interface to a firewall. See Anti-overbilling with FortiOS Carrier.
Gn	SGSN and external SGSNs and internal GGSNs	GTP	When the GTP tunnel is deleted, need to inform other interfaces immediately to prevent misuse of connections remaining open. FortiOS Carrier adds this interface to a firewall.
Gp	Internal SGSN and external GGSNs	GTP	
Gz	GSN (SGSN and GGSN) and the charging gateway (CG)	GTP'	Used for the offline charging interface. Ga is used for online charging.

Corporate customers may have a direct connection to the Gi interface for higher security. The Gi interface is normally an IP network, though a tunnelling protocol such as GRE or IPsec may be used instead.

Packet flow through the GPRS network

To better understand the GPRS network, we will follow the path data takes for a normal connection. For this example a call placed from a mobile phone involves accessing services on the Internet.

Sample GPRS network topology



1. A mobile phone places a call using a mobile station (MS). This connection between the mobile phone and the MS is a radio connection using one of the radio access technologies. See Radio Access Technology (RAT) type.
2. The MS connects to a GPRS System Node (GSN) specifically a Sending GSN. This connection uses the Gb interface and typically uses IP address or Frame Relay.
3. The SGSN checks the mobile phone information located in the home location register (HLR) or visitor location register (VLR) to ensure there is subscriber information for that phone. If this mobile phone is from another network, the SGSN uses the VLR and updates its home carrier's information with its current location and information. This connection involves the Ga or Gz interfaces, and uses the GTP' protocol for communication.
4. The SGSN checks to make sure the phone did not transfer this connection from a different MS. If it did, the connection has already been established (along with the billing) and is handed off to this SGSN. If the call is being handed over from another SGSN, it will use the Gn interface between the two SGSNs.
5. The SGSN sends GTP messages to the local external Gateway GSN (GGSN) to create a GTP tunnel for this PDP context to access the Internet. It is possible that a remote GGSN has access to a service, such as a WAP gateway, that the local GGSN is missing. In this situation, the local SGSN uses the Gp interface to connect to the remote GGSN. Both the Gn and Gp interfaces use GTP.
6. The both the local and remote GGSNs connect to external services outside the GPRS network. These services can include a WAP gateway, a corporate IP network directly connected to the GPRS network, or the Internet. The connection from the GGSN to the external services uses the Gi interface.

SCTP

As of FortiOS version 5.0, the FortiGate natively handles SCTP (Stream Control Transport Protocol) traffic, as an alternative to TCP and UDP for use in Carrier networks. The FortiGate handles SCTP as if it would any other traffic.

Overview

SCTP is a connection-oriented transport protocol that overcomes some of the limitations of both TCP and UDP that prevent reliable transfer of data over IP-based networks (such as those used by telephony systems and carrier networks). The 'Stream' in SCTP refers to the sequence of user messages or packets that are considered at the same time to be individual objects and also treated as a whole by networked systems. SCTP is less vulnerable to congestion and flooding due to more advanced error handling and flood protection built into the protocol.

SCTP features as compared to TCP and UDP

Feature	SCTP	TCP	UDP
State required at each endpoint	yes	yes	no
Reliable data transfer	yes	yes	no
Congestion control and avoidance	yes	yes	no
Message boundary conservation	yes	no	yes
Path MTU discovery and message fragmentation	yes	yes	no
Message bundling	yes	yes	no
Multi-homed hosts support	yes	no	no
Multi-stream support	yes	no	no
Unordered data delivery	yes	no	yes
Security cookie against SYN flood attack	yes	no	no
Built-in heartbeat (reachability check)	yes	no	N/A

All of these features are built into the design of the Protocol, and the structure of SCTP packets and networks. The FortiGate unit interprets the traffic and provides the necessary support for maintenance and verification features, but the features are not FortiGate specific. These features are documented in greater detail below.

State required at each endpoint

Constant back and forth acknowledgement and content verification messages are sent between all SCTP peer endpoints, and all endpoints' state machine actions must be synchronized for traffic to flow.

Reliable data transfer

SCTP places data and control information (eg. source, destination, verification) into separate messages, both sharing the same header in the same SCTP packet. This allows for constant verification of the contained data at both ends and along the path, preventing data loss or fragmentation. As well, data is not sent in an interruptible stream as in TCP.

Congestion control and avoidance

Built-in, constantly updating path detection and monitoring automatically redirect packets along alternate paths in case of traffic congestion or inaccessible destinations. For deliberate/malicious congestion control, see the below section on Security cookie against SYN flood attack.

Message boundary conservation

SCTP is designed in such a way that no matter how messages are divided, redirected, or fragmented, the message boundaries will be maintained within the packets, and all messages cannot be appended without tripping verification mechanisms.

Path MTU discovery and message fragmentation

SCTP is capable of Path Maximum Transmission Unit discovery, as outlined in RFC4821. Two specific alterations have been made to how SCTP handles MTU. First, that endpoints will have separate MTU estimates for each possible multi-homed endpoint. Second, that bundled message fragments (as explained below) will be directed based on MTU calculations, so that retransmissions (if necessary) will be sent without delay to alternate addresses.

Message bundling

SCTP is a message-oriented protocol, which means that despite being a streaming data protocol, it transports a sequence of specific messages, rather than transporting a stream of bytes (like TCP). Since some data transmissions are small enough to not require a complete message's worth of content, so multiple pieces of content will be transmitted simultaneously within the messages.

Multi-homed hosts support

SCTP supports multi-homing, which is a network structure in which one or multiple sources/destinations has more than one IP address. SCTP can adapt to multi-homing scenarios and redirect traffic to alternate IP addresses in case of failure.

Multi-stream support

Due to the message bundling feature allowing for multiple pieces of content to be sent in messages at once, SCTP can 'multi-stream' content, by deliberately dividing it among messages at a fixed rate, so that multiple types of content (eg. both images and text) can be loaded at once, at the same pace.

Unordered data delivery

With control messages in every packet to provide verification of any packet's data and its place in the stream, the data being transmitted can actually arrive in any order, and verify that all has arrived or that some is missing.

Security cookie against SYN flood attack

Since every packet contains verification of its place in the stream, it makes it easy for the protocol to detect when redundant, corrupted or malicious packets flood the path, and they are automatically dropped when necessary.

Built-in heartbeat (reachability check)

Endpoints automatically send specific control chunks among the other SCTP packet information to peer endpoints, to determine the reachability of the destination. Hearthbeat acknowledgement packets are returned if the destination is available.

SCTP Firewall

FortiGate stateful firewalls will protect and inspect SCTP traffic, according to RFC4960. SCTP over IPsec VPN is also supported. The FortiGate device is inserted as a router between SCTP endpoints. It checks SCTP Syntax for the following information:

- Source and destination port
- Verification Tag
- Chunk type, chunk flags, chunk length
- Sequence of chunk types
- Associations

The firewall also oversees and maintains several SCTP security mechanisms:

- SCTP four-way handshake
- SCTP heartbeat
- NAT over SCTP

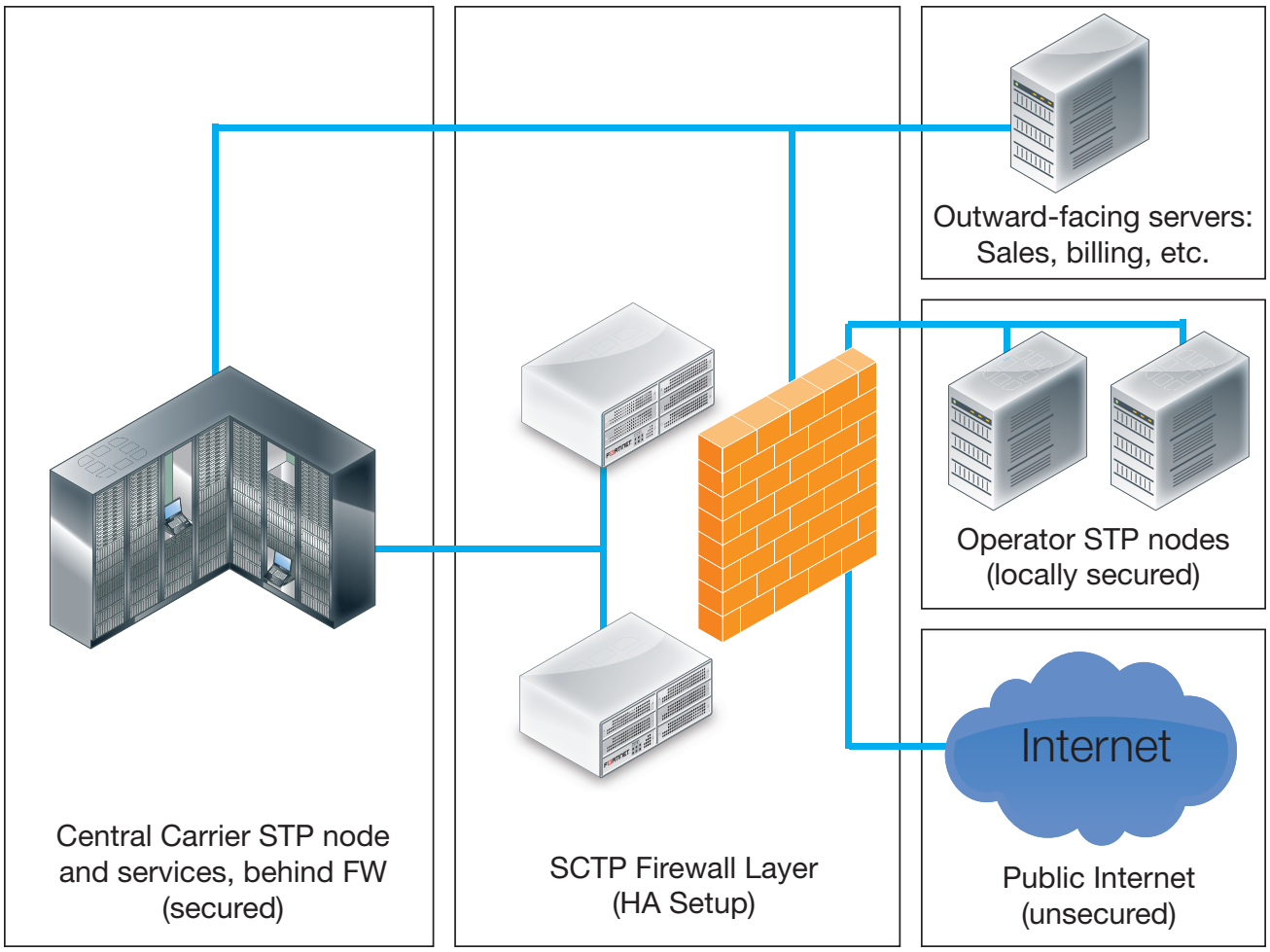
The firewall has IPS DoS protection against known threats to SCTP traffic, including INIT/ACK flood attacks, and SCTP fuzzing.

SCTP example scenario

An ideal SCTP configuration for a Carrier serving multiple operators/service providers involves a unified Firewall, securing all incoming and outgoing traffic over the Carrier network, whether it be standard web traffic, GTP or other carrier traffic, or corporate traffic for the Carrier company.

One best practice method to provide a unified firewall with built-in redundancy is to make use of multiple FortiGate units, connected in a High Availability cluster. Also, there are additional methods that can be applied to ease the complexity of managing multiple services, functions, and traffic types across multiple devices.

Sample SCTP Network Topology

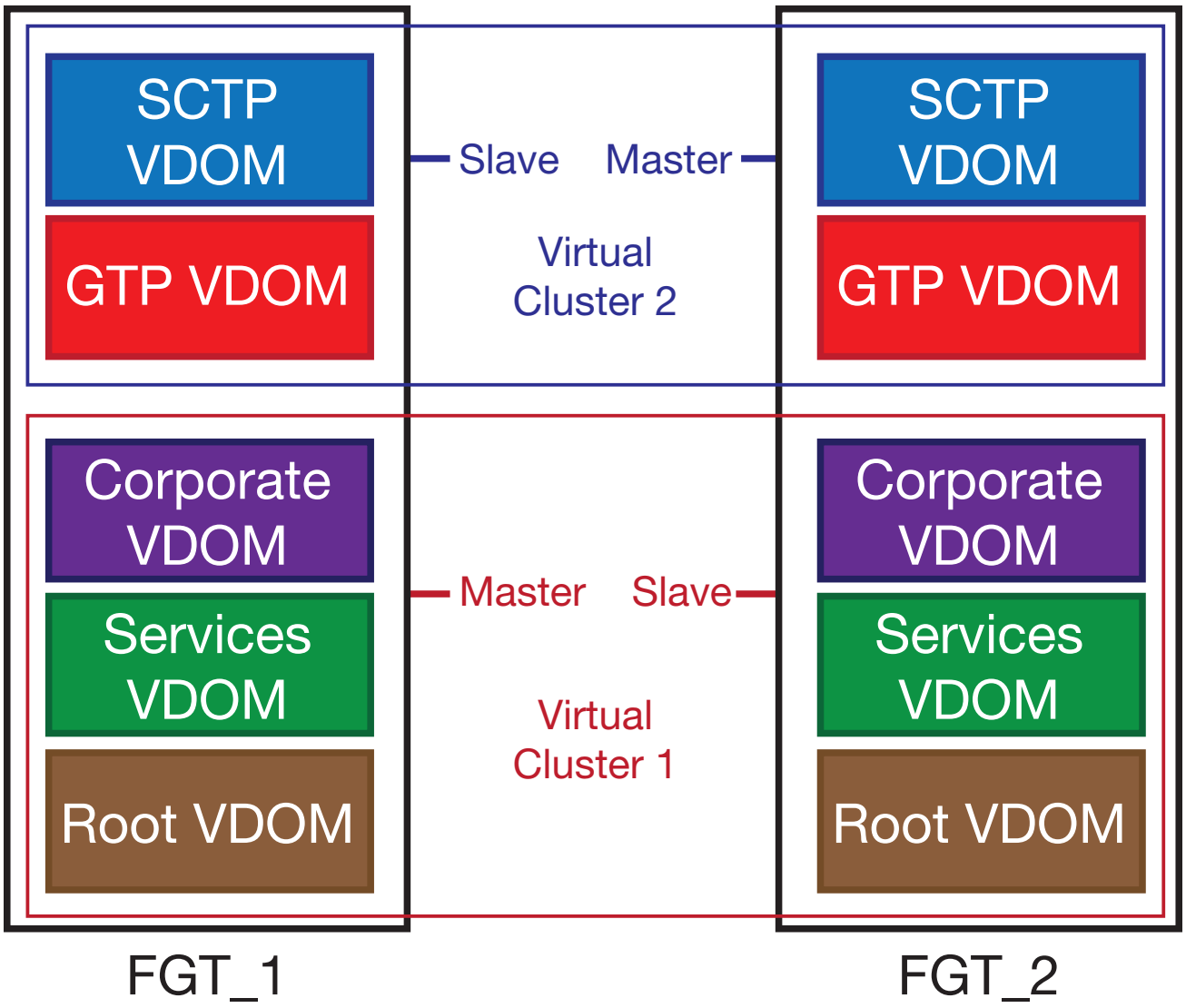


In this example, the firewall layer is configured with two FortiGate devices to act as an HA cluster, providing automatic load balancing and failover detection for the main firewall.

The two devices together make up the firewall, through which all traffic passes. Virtual Domains are created within the FortiGate units, distributing services and traffic into individual VDOMs, allowing them to be monitored and secured individually, to help mitigate possible threats to Carrier networks that target specific services. Individual departments or administrators can manage specific VDOMs, or the FortiGates can be collectively managed centrally by network administrators.

The VDOMs are distributed as shown below:

VDOM distribution between SCTP Firewall Layer FortiGate units



One FortiGate handles basic FortiGate services and non-Carrier traffic. Configuring virtual clustering across the two FortiGates allows one to mirror its VDOMs across to the other unit.

The second FortiGate can then primarily provide Carrier-specific services and handle SCTP, Gi and GTP traffic, using the first FortiGate as the slave unit in a second virtual cluster.

Carrier web-based manager settings

The Carrier menu provides settings for configuring FortiOS Carrier features within the Security Profiles menu. These features include MMS and GTP profiles.

In **Security Profiles > Carrier**, you can configure profiles and settings for MMS and GTP. In the Carrier menu, you can configure an MMS profile and then apply it to a security policy. You can also configure GTP profiles and apply those to security policies as well.

This topic includes the following:

MMS profiles

Since MMS profiles can be used by more than one security policy, you can configure one profile for the traffic types handled by a set of security policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

If the security policy requires authentication, do not select the MMS profile in the security policy. This type of profile is specific to the authenticating user group. For details on configuring the profile associated with the user group, see User Groups in the Authentication guide.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate protection profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

Once you have configured the MMS profile, you can then apply the profile to MMS traffic by applying it to a security policy.

MMS profiles can contain settings relevant to many different services. Each security policy uses the subset of the MMS profile settings that apply to the sessions accepted by the security policy. In this way, you might define just one MMS profile that can be used by many security policies, each policy using a different or overlapping subset of the MMS profile.

The MMS Profile page contains options for each of the following:

- MMS scanning
- MMS Bulk Email Filtering Detection
- MMS Address Translation
- MMS Notifications
- DLP Archive
- Logging

MMS profile configuration settings

The following are MMS profile configuration settings in **Security Profiles > Carrier > MMS Profile**.

MMS Profile page Lists each individual MMS profile that you created. On this page, you can edit, delete or create an MMS profile.	
Create New	Creates a new MMS profile. When you select **Create New**, you are automatically redirected to the New MMS Profile page.
Edit	Modifies settings within an MMS profile. When you select **Edit**, you are automatically redirected to the Edit MMS Profile.
Delete	Removes an MMS profile from the list on the MMS Profile page. To remove multiple MMS profiles from within the list, on the MMS Profile page, in each of the rows of the profiles you want removed, select the check box and then select **Delete**. To remove all MMS profiles from the list, on the MMS Profile page, select the check box in the check box column, and then select **Delete**.
Name	The name of the MMS profile.
Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (**Security Profiles > Antivirus > Profiles**), 1 appears in **Ref.** . To view the location of the referenced object, select the number in **Ref.**, and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is avialable within the Object Usage window: **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page. **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.

New MMS Profile page	
Provides settings for configuring an MMS profile. This page also provides settings for configuring DLP archives and logging.	
Profile Name	Enter a name for the profile.
Comments	Enter a description about the profile. This is optional.
MMS Scanning	Configure MMS Scanning options.
MMS Bulk Email Filtering Detection	Configure MMS Bulk Email options.
MMS Address Translation	Configure MMS Address Translation options.
MMS Notifications	Configure MMS Notification options.
DLP Archive	Configure DLP archive option.
Logging	Configure logging options.

MMS scanning options

You can configure MMS scanning protection profile options to apply virus scanning, file filtering, content filtering, carrier endpoint blocking, and other scanning to MMS messages transmitted using the MM1, MM3, MM4 and MM7 protocols.

The following are the MMS Scanning options that are available within an MMS profile. You can create an MMS profile in **Security Profiles > Carrier > MMS Profile** or edit an existing one. You must expand MMS Scanning to access the following options.

MMS Scanning section of the New MMS Profile page	
Monitor Only	Select to cause the unit to record log messages when MMS scanning options find a virus, match a file name, or match content using any of the other MMS scanning options. Select this option to be able to report on viruses and other problems in MMS traffic without affecting users. **Tip:** Select **Remove Blocked** if you want the unit to actually remove content intercepted by MMS scanning options.
Virus Scan	Select to scan attachments in MMS traffic for viruses. Since MM1 and MM7 use HTTP, the oversize limits for HTTP and the HTTP antivirus port configuration also applies to MM1 and MM7 scanning. MM3 and MM4 use SMTP and the oversize limits for SMTP and the SMTP antivirus port configuration also applies to MM3 and MM4 scanning.
Scan MM1 message retrieval	Select to scan message retrievals that use MM1. If you enable **Virus Scan** for all MMS interfaces, messages are also scanned while being sent. In this case, you can disable MM1 message retrieval scanning to improve performance.
Quarantine	Select to quarantine the selected MMS traffic
Remove Blocked	Select to remove blocked content from each protocol and replace it with the replacement message. Select **Constant** if the unit is to preserve the length of the message when removing blocked content, as may occur when billing is affected by the length of the message. **Tip:** If you only want to monitor blocked content, select **Monitor Only**.
Content Filter	Select to filter messages based on matching the content of the message with the words or patterns in the selected web content filter list. For information about adding a web content filter list, see the FortiGate CLI Reference.
Carrier Endpoint Block	Select to add **Carrier Endpoint Filtering** in this MMS profile. Select the carrier endpoint filter list to apply it to the profile.
MMS Content Checksum	Select to add MMS Content Checksum in this MMS profile. Select the MMS content checksum list to apply it to the profile.

MMS Scanning section of the New MMS Profile page	
Pass Fragmented Messages	Select to pass fragmented MM3 and MM4 messages. Fragmented MMS messages cannot be scanned for viruses. If you do not select these options, fragmented MM3 and MM4 message are blocked.
Comfort Clients	Select client comforting for MM1 and MM7 sessions. Since MM1 and MM7 messages use HTTP, MM1 and MM7 client comforting operates like HTTP client comforting.
Comfort Servers	Select server comforting for each protocol. Similar to client comforting, you can use server comforting to prevent server connection timeouts that can occur while waiting for the unit to buffer and scan large POST requests from slow clients.
Interval (1-900 seconds)	Enter the time in seconds before client and server comforting starts after the download has begun, and the time between sending subsequent data.
Amount (1-10240 bytes)	The number of bytes sent by client or server comforting at each interval.
Oversized MMS Message	Select **Block** or **Pass** for files and email messages exceeding configured thresholds for each protocol. The oversize threshold refers to the final size of the message, including attachments, after encoding by the client. Clients can use a variety of encoding types; some result in larger file sizes than the original attachment. As a result, a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the oversize threshold.
Threshold (1KB - 800 MB)	Enter the oversized file threshold and select KB or MB. If a file is larger than the threshold the file is passed or blocked depending on the ***Oversized MMS Message*** setting. The web-based manager displays the allowed threshold range. The threshold maximum is 10% of the unit's RAM.

MMS bulk email filtering options

You can use the MMS bulk email filtering options to detect and filter MM1 and MM4 message floods and duplicate messages. You can configure three thresholds that define a flood of message activity and three thresholds that define excessive duplicate messages. The configuration of each threshold includes the response actions for the threshold.

The configurable thresholds for each of the flood and duplicate sensors and must be enabled in sequence. For example, you can enable Flood Threshold 1 and Flood Threshold 2, but you cannot disable Flood Threshold 1 and enable Flood Threshold 2.

You can also add MSISDN to the bulk email filtering configuration and select a subset of the bulk email filtering options to applied to these individual MSISDNs.

You must first select MM1 and/or MM4 to detect excessive message duplicates. If excessive message duplicates are detected, the unit will perform the **Duplicate Message Action** for the specified duration.

You can configure three duplicate message thresholds and enable them with separate values and actions. They are labeled Duplicate Threshold 1 through 3 and must be enabled in sequence. For example, you can enable Duplicate Threshold 1 and Duplicate Threshold 2, but you cannot disable Duplicate Threshold 1 and enable Duplicate Threshold 2.

When traffic accepted by a security policy that contains an MMS profile with duplicate message configured receives MM1 or MM4 duplicate messages that match a threshold configured in the MMS protection profile, the unit performs the duplicate message action configured for the matching threshold.

You can configure three message flood thresholds and enable them with separate values and actions. They are labeled Flood Threshold 1 through 3 and must be enabled in sequence. For example, you can enable Flood Threshold 1 and Flood Threshold 2, but you cannot disable Flood Threshold 1 and enable Flood Threshold 2.

When traffic accepted by a security policy that contains an MMS protection profile with message flooding configured experiences MM1 or MM4 message flooding that matches a threshold configured in the MMS profile, the unit performs the message flood action configured for the matching threshold.

MMS Bulk Email Filtering Detection

This section of the New MMS Profile page contains numerous sections where you can configure specific settings for flood threshold, duplicate threshold and recipient MSISDNs.

Message Flood

The message flood settings for each flood threshold. Expand each to configure settings for a threshold.

Flood Threshold 1	Expand to reveal the flood threshold settings for Flood Threshold 1. The settings for Flood Threshold 1 are the same for Flood Threshold 2 and 3.
Enable	Select to apply Flood Threshold 1 to the MSISDN exception.
Message Flood Window	Enter the period of time during which a message flood will be detected if the **Message Flood Limit** is exceeded. The message flood window can be 1 to 2880 minutes (48 hours).
Message Flood Limit	Enter the number of messages which signifies a message flood if exceeded within the **Message Flood Window**.
Message Flood Block Time	Enter the amount of time during which the unit performs the **Message Flood Action** after a message flood is detected.
Message Flood Action	Select one or more actions that the unit is to perform when a message flood is detected.
Flood Threshold 2	Expand to configure settings for Flood Threshold 2 or 3 respectively.
Flood Threshold 3	

Duplicate Message

The duplicate message threshold settings. Expand each to configure settings for a threshold.

MM1 Retrieve Duplicate Enable	Select to scan MM1 `mm1-retr` messages for duplicates. By default, `mm1-retr` messages are not scanned for duplicates as they may often be the same without necessarily being bulk or spam.
Enable	Select to enable the selected duplicate message threshold and to make the rest of the options available for configuration.
Duplicate Message Window	Enter the period of time during which excessive message duplicates will be detected if the Duplicate message Limit it exceeded. The duplicate message window can be 1 to 2880 minutes (48 hours).
Duplicate Message Limit	Enter the number of messages which signifies excessive message duplicates if exceeded within the Duplicate Message Window.

Duplicate Message Block Time	Enter the amount of time during which the unit will perform the Duplicate Message Action after a message flood is detected.
Duplicate Message Action	Select one or more actions that the unit is to perform when excessive message duplication is detected.
Duplicate Threshold 2	Expand to configure settings for Duplicate Threshold 2 or 3 respectively.
Duplicate Threshold 3	

Recipient MSISDN

The recipient Mobile Subscriber Integrated Services Digital Network Number (MSISDN) settings for each recipient MSISDN. When you select **Create New**, you are automatically redirected to the New MSISDN page.

You need to save the profile before you can add MSISDNs.

Recipient MSISDN	The recipient MSISDN.
Flood Threshold 1	Check to enable Flood Threshold 1 settings for this MSISDN.
Flood Threshold 2	ICheck to enable Flood Threshold 2 settings for this MSISDN..
Flood Threshold 3	ICheck to enable Flood Threshold 3 settings for this MSISDN..
Duplicate Threshold 1	Check to enable Duplicate Threshold 1 settings for this MSISDN..
Duplicate Threshold 2	Check to enable Duplicate Threshold 2 settings for this MSISDN..
Duplicate Threshold 3	Check to enable Duplicate Threshold 3 settings for this MSISDN..
Edit	Modifies the settings of a Recipient MSISDN in the Recipient MSISDN list. When you select **Edit**, you are automatically redirected to the New MSISDN page.
Delete	Removes a Recipient MSISDN in the Recipient MSISDN list within the Recipient MSISDN section of the page.

New MSISDN page

Create New	Creates a new Recipient MSISDN. When you select **Create New**, you are automatically redirected to the New MSISDN page.
Recipient MSISDN	Enter a name for the recipient MSISDN.
Flood Threshold 1	Select to apply Flood Threshold 1 to the MSISDN exception.
Flood Threshold 2	Select to apply Flood Threshold 2 to the MSISDN exception.

Flood Threshold 3	Select to apply Flood Threshold 3 to the MSISDN exception.
Duplicate Threshold 1	Select to apply Duplicate Threshold 1 to the MSISDN exception.
Duplicate Threshold 2	Select to apply Duplicate Threshold 2 to the MSISDN exception.
Duplicate Threshold 3	Select to apply Duplicate Threshold 3 to the MSISDN exception.

MMS Address Translation options

The sender’s carrier endpoint is used to provide logging and reporting details to the mobile operator and to identify the sender of infected content.

When MMS messages are transmitted, the **From** field may or may not contain the sender's address. When the address is not included, the sender information will not be present in the logs and the unit will not be able to notify the user if the message is blocked unless the sender's address is made available elsewhere in the request.

The unit can extract the sender's address from an extended HTTP header field in the HTTP request. This field must be added to the HTTP request before it is received by the unit. If this field is present, it will be used instead of the sender's address in the MMS message for logging and notification. If this header field is present when a message is retrieved, it will be used instead of the **To** address in the message. If this header field is not present the content of the **To** header field is used instead.

Alternatively, the unit can extract the sender’s address from a cookie.

You can configure MMS address translation to extract the sender’s carrier endpoint so that it can be added to log and notification messages. You can configure MMS address translation settings to extract carrier endpoints from HTTP header fields or from cookies. You can also configure MMS address translation to add an endpoint prefix to the extracted carrier endpoints. For more information, see Dynamic Profiles and Endpoints in the Authentication guide.

MMS Address Translation	
Sender Address Source	Select to extract the sender's address from the **HTTP Header Field** or a **Cookie**. You must also specify the identifier that contains the carrier endpoint.

Sender Address Identifier	Enter the sender address identifier that includes the carrier endpoint. The default identifier is `x-up-calling-line-id`.
	
	If the **Sender Address Source** is **HTTP Header Field**, the address and its identifier in the HTTP request header takes the format:
	
	`<Sender Address Identifier>: <MSISDN_value>`
	
	Where the `<MSISDN_value>` is the carrier endpoint. For example, the HTTP header might contain:
	
	`x-up-calling-line-id: 6044301297`
	
	where `x-up-calling-line-id` would be the Sender Address Identifier.
	
	If the **Sender Address Source** is Cookie, the address and its identifier in the HTTP request header's `Cookie` field takes the format of attribute-value pairs:
	
	`Cookie: id=<cookie-id>;`
	
	`<Sender Address Identifier>=<MSISDN Value>`
	
	For example, the HTTP request headers might contain:
	
	`Cookie: id=0123jf!a;x-up-calling-line-id=6044301297`
	
	where `x-up-calling-line-id` would be the **Sender Address Identifier**.

Convert Sender Address From / To HEX	Select to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications.
Add Carrier Endpoint Prefix for Logging / Notification	Select the following to enable adding endpoint prefixes for logging and notification.
Enable	Select to enable adding the country code to the extracted carrier endpoint, such as the MSISDN, for logging and notification purposes. You can limit the number length for the test numbers used for internal monitoring without a country code.

MMS Address Translation	
Prefix	Enter a carrier endpoint prefix to be added to all carrier endpoints. Use the prefix to add extra information to the carrier endpoint in the log entry.
Minimum Length	Enter the minimum length of the country code information being added. If this and Maximum Length are set to zero (0), length is not limited.
Maximum Length	Enter the maximum length of the country code information being added. If this and Minimum Length are set to zero (0), length is not limited.

MMS Notifications

MMS notifications are messages that a unit sends when an MMS profile matches content in an MM1, MM3, MM4 or MM7 session. For example, the MMS profile detects a virus or uses content blocking to block a web page, text message or email. You can send notifications to the sender of the message using same protocol and the addressing headers in the original message. You can also configure MMS notifications to send notification messages to another destination (such as a system administrator) using the MM1, MM3, MM4 or MM7 protocol.

You need to enable one or more **Notification Types** or you can add an **Antivirus Notification List** to enable sending notifications,.

You can also use MMS notifications options to configure how often notifications are sent. The unit sends notification messages immediately for the first event, then at a configurable interval if events continue to occur. If the interval does not coincide with the window of time during which notices may be sent, the unit waits to send the notice in the next available window. Subsequent notices contain a count of the number of events that have occurred since the previous notification.

There are separate notifications for each notification type, including virus events. Virus event notifications include the virus name. Up to three viruses are tracked for each user at a time. If a fourth virus is found, one of the existing tracked viruses is removed from the list.

The notifications are MM1 `m-send-req` messages sent from the unit directly to the MMSC for delivery to the client. The host name of the MMSC, the URL to which `m-send-req` messages are sent, and the port must be specified.

MMS Notification	
Antivirus Notification List	Optionally select an antivirus notification list to select a list of virus names to send notifications for. The unit sends a notification message whenever a virus name or prefix in the antivirus notification list matches the name of a virus detected in a session scanned by the MMS protection profile. Select **Disabled** if you do not want to use a notification list. Instead of selecting a notification list you can configure the **Virus Scan Notification Type** to send notifications for all viruses.
Message Protocol	In each column, select the protocol used to send notification messages. You can use a different protocol to send the notification message than the protocol on which the violation was sent. The MMS Notifications options change depending on the message protocol that you select. If you select a different message protocol, you must also enter the User Domain. If selecting MM7 you must also enter the Message Type.
Message Type	Select the MM7 message type to use if sending notifications using MM7. Options include deliver.REQ and submit.REQ
Detect Server Details	Select to use the information in the headers of the original message to set the address of the notification message. If you do not select this option, you can enter the required addressing information manually. You cannot select **Detect Server Details** if you are sending notification messages using a different message protocol. If you select **Detect Server Details**, you cannot change the **Port** where the notification is being sent.
Hostname	Enter the FQDN or the IP address of the server where the notifications will be sent.
URL	Enter the URL of the server. For example if the notificaiton is going to www.example.com/home/alerts , the URL is /home/alerts. This option is available only when **Message Protocol** is **mm1** or **mm7**.
Port	Enter the port number of the server. You cannot change the ***Port*** if ***Detect Server Details*** is enabled.

MMS Notification	
Username	Enter the user name required for sending messages using this server (optional). This option is available only when **Message Protocol** is **mm7**.
Password	Enter the password required for sending messages using this server (optional). This option is available only when **Message Protocol** is **mm7**.
VASP ID	Enter the value-added-service-provider (VASP) ID to be used when sending a notification message. If a VAS is not offered by the mobile provider, it is offered by a third party or a VAS provider or content provider (CP). This option is available only when **Message Protocol** is **mm7**.
VAS ID	Enter the value-added-service (VAS) ID to be used when sending a notification message. A VAS is generally any service beyond voice calls and fax. This option is available only when **Message Protocol** is **mm7**.
All Notification Types	In each column, select notification for all MMS event types for that MMS protocol, then enter the amount of time and select the time unit for notice intervals. Alternatively, expand **All Notification Types**, and then select notification for individual MMS event types for each MMS protocol. Then enter the amount of time and select the time unit for notice intervals. Not all event types are available for all MMS protocols.
Content Filter	In each column, select to notify when messages are blocked by the content filter, then enter the amount of time and select the time unit for notice intervals.
File Block	In each column, select to notify when messages are blocked by file block, then enter the amount of time and select the time unit for notice intervals.
Carrier Endpoint Block	In each column, select to notify when messages are blocked, then enter the amount of time and select the time unit for notice intervals.
Flood	In each column, select to notify when message flood events occur, then enter the amount of time and select the time unit for notice intervals.

MMS Notification	
Duplicate	In each column, select to notify when duplicate message events occur, then enter the amount of time and select the time unit for notice intervals.
MMS Content Checksum	In each column, select to notify when the content within an MMS message is scanned and banned because of the checksum value that was matched.
Virus Scan	In each column, select to notify when the content within an MMS message is scanned for viruses.
Notifications Per Second Limit	For each MMS protocol, enter the number of notifications to send per second. If you enter zero (0), the notification rate is not limited.
Day of Week	For each MMS protocol, select the days of the week the unit is allowed to send notifications.
Window Start Time	For each MMS protocol, select the time of day to begin the message alert window. By default, the message window starts at 00:00. You can change this if you want to start the message window later in the day. When configured, notification outside this window will not be sent.
Window Duration	For each MMS protocol, select the time of day at which to end the message alert window. By default, the message window ends at 00:24. You can change this if you want to end the message window earlier in the day. When configured, notification outside this window will not be sent

DLP Archive options

Select DLP archive options to archive MM1, MM3, MM4, and MM7 sessions. In addition to the MMS profile's DLP archive options, you can:

- Archive MM1 and MM7 message floods
- Archive MM1 and MM7 duplicate messages
- Select **DLP archiving** for carrier endpoint patterns in a **Carrier Endpoint List** and select the **Carrier Endpoint Block** option in the **MMS Scanning** section of an MMS Profile

The unit only allows one sixteenth of its memory for transferring content archive files. For example, for units with 128MB RAM, only 8MB of memory is used when transferring content archive files. Best practices dictate to not enable full content archiving if antivirus scanning is also configured because of these memory constraints.

DLP Archive	
Display DLP meta-information on the system dashboard	Select each required protocol to display the content archive summary in the Log and Archive Statistics dashboard widget on the System Dashboard.
Archive to FortiAnalyzer/FortiGuard	Select the type of archiving that you want for the protocol (MM1, MM3, MM4, and MM7). You can choose from Full, Summary or None. **None —** Do not send content archives. **Summary —** Send content archive metadata only. Includes information such as date and time, source and destination, request and response size, and scan result. **Full —** Send content archive both metadata and copies of files or messages. In some cases, FortiOS Carrier may not archive content, or may make only a partial content archive, regardless of your selected option. This behavior varies by prerequisites for each protocol. This option is available only if a FortiAnalyzer unit or FortiGuard Analysis and Management Service is configured.

Logging

You can enable logging in an MMS profile to write event log messages when the MMS profile options that you have enabled perform an action. For example, if you enable MMS antivirus protection, you could also use the MMS profile logging options to write an event log message every time a virus is detected.

You must first configure how the unit stores log messages so that you can then record these logs messages. For more information, see the FortiOS Handbook Logging and Reporting guide.

Logging	
MMS-Antivirus	If antivirus settings are enabled for this MMS profile, select the following options to record **Antivirus Log** messages.
Viruses	Record a log message when this MMS profile detects a virus.
Blocked Files	Record a log message when antivirus file filtering enabled in this MMS profile blocks a file.
Intercepted Files	Record a log message when this MMS profile intercepts a file.
Oversized Files/E-mails	Record a log message when this MMS profile encounters an oversized file or email message. Oversized files and email messages cannot be scanned for viruses.
MMS Scanning	If MMS scanning settings are enabled for this MMS profile, select the following options to record **Email Filter Log** messages.
Notification Messages	Select to log the number of MMS notification messages sent.
Bulk Messages	Select to log MMS Bulk AntiSpam events. You must also select which protocols to write log messages for in the MMS bulk email filtering part of the MMS profile.
Carrier Endpoint Filter Block	Select to log MMS carrier endpoint filter events, such as MSISDN filtering.
MMS Content Checksum	Select to log MMS content checksum activity.
Content Block	Select to log content blocking events.

MMS Content Checksum

The MMS Content Checksum menu allows you to configure content checksum lists.

Configure MMS content checksum lists in **Security Profiles > Carrier > MMS Content Checksum** using the following table.

MMS Content Checksum Lists each individual content checksum list that you created. On this page, you can edit, delete or create a content checksum list.	
Create New	Creates a new MMS content checksum list. When you select **Create New**, you are automatically redirected to the New List. This page provides a name field and comment field. You must enter a name to go to MMS Content Checksum Settings page.
Edit	Modifies settings to a MMS content checksum. When you select **Edit**, you are automatically redirected to the MMS Content Checksum Settings page.
Delete	Removes an MMS content checksum from the page. To remove multiple content checksum lists from within the list, on the MMS Content Checksum page, in each of the rows of the content checksum lists you want removed, select the check box and then select **Delete**. To remove all content checksum lists from list, on the MMS Content Checksum page, select the check box in the check box column and then select **Delete**.
Name	The name of the MMS content checksum list that you created.
# Entries	The number of checksums that are included in the content checksum list.
MMS Profiles	The MMS profile or profiles that have the MMS content checksum list applied. For example if two different MMS profiles use this content checksum list, they will both be listed here.
Comments	A description given to the MMS content checksum.

Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (**Security Profiles > AntiVirus > Profiles**), 1 appears in **Ref.** . To view the location of the referenced object, select the number in **Ref.**, and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is avialable within the Object Usage window: • **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. • **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.

Notification List

The Notification List menu allows you to configure a list of viruses. This virus list provides a list for scanning viruses in MMS messages. You can use one virus list in multiple MMS profiles, and configure multiple virus lists.

Notification list configuration settings

The following are notification list configuration settings in **Security Profiles > Carrier > Notification List**.

Notification List Lists all the notification lists that you created. On this page you can edit, delete or create a new notification list.	
Create New	Creates a new notification list. When you select **Create New**, you are automatically redirected to the New List page. You must enter a name to go to the Notification List Settings page.
Edit	Modifies settings within the notification list. When you select **Edit**, you are automatically redirected to the Notification List Settings page.
Delete	Removes a notification list from the list on the Notification List page. To remove multiple notification lists from within the list, on the Notification List page, in each of the rows of the notification lists you want removed, select the check box and then select **Delete**. To remove all notification lists from the list, on the Notification List page, select the check box in the check box column and then select **Delete**.
Name	The name of the MMS content checksum list that you created.
# Entries	The number of checksums that are included in that content checksum list.
MMS Profiles	The MMS profile or profiles that are associated with
Comments	A description given to the MMS notification list.

Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (**Security Profiles > Antivirus > Profiles**), 1 appears in **Ref.** . To view the location of the referenced object, select the number in **Ref.**, and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is avialable within the Object Usage window: • **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. • **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.

Notification List Settings

Provides settings for configuring a notification list, which is a list of viruses and is used for scanning viruses in MMS messages. This list is called the Antivirus Notification List in an MMS profile.

Name	If editing the name of a notification list, enter the new name in this field. You must select **OK** to save the change.
Comments	If you want to enter a comment, enter the comment in the field. You must select **OK** to save the change.
Create New	Creates a notification entry in the list. When you select **Create New**, you are automatically redirected to the New Entry page.
Edit	Modifies settings within a notification list. When you select **Edit**, you are automatically redirected to the Edit Entry page.

Delete	Removes a notification entry from the list on the page. To remove multiple notification entries from within the list, on the Notification List Settings page, in each of the rows of the entries you want removed, select the check box and then select **Delete**. To remove all notification entries from the list, on the Notification List Settings page, select the check box in the check box column and then select **Delete**.
Enable	Enables a notification entry that is disabled.
Disable	Disables a notification entry so that it is not active and available for use, but it is not deleted.
Remove All Entries	Removes all notification entries that are listed on the Notification List Settings page.
Enable	Displays whether or not the checksum is enabled.
Virus Name/Profile	The name of the virus that was added to the list.
Entry Type	The type of match that will be used to match the virus stated in the notification list to the actual virus that is found.
New Entry page	
Virus Name/Profile	Enter the virus name.
Entry Type	Select the type of match that will be used to match the virus stated in the notification list to the actual virus that is found.
Enable	Select to enable the virus in the list.

Message Flood

The convenience offered by MM1 and MM4 messaging can be abused by users sending spam or attempting to overload the network with an excess of messages. MMS flood prevention can help prevent this type of abuse. A message flood occurs when a single subscriber sends a volume of messages that exceed the flood threshold that you set. The threshold defines the maximum number of messages allowed, the period during which the subscriber sent messages are considered, and the length of time the sender is restricted from sending messages after a flood is detected. For example, for the first threshold you may determine that any subscriber who sends more than 100 MM1 messages in an hour (60 minutes) will have all outgoing messages blocked for 30 minutes.

Action	Description
Log	Add a log entry indicating that a message flood has occurred. You must also enable logging for **MMS Scanning > Bulk Messages** in the **Logging** section of the MMS protection profile.
DLP Archive	Save the first message to exceed the flood threshold, or all the messages that exceed the flood threshold, in the DLP archive. DLP archiving flood messages may not always produce useful results. Since different messages can be causing the flood, reviewing the archived messages may not be a good indication of what is causing the problem since the messages could be completely random.
All messages	All the messages that exceed the flood threshold will be saved in the DLP archive.
First message only	Save only the first message to exceed the flood threshold in the DLP archive. Other messages in the flood are not saved. For message floods this may not produce much useful information since a legitimate message could trigger the flood threshold.
Intercept	Messages that exceed the flood threshold are passed to the recipients, but if quarantine is enabled for intercepted messages, a copy of each message will also quarantined for later examination. If the quarantine of intercepted messages is disabled, the **Intercept** action has no effect.
Block	Messages that exceed the flood threshold are blocked and will not be delivered to the message recipients. If quarantine is enabled for blocked messages, a copy of each message will quarantined for later examination.
Alert Notification	If the flood threshold is exceeded, the Carrier-enabled FortiGate unit will send an MMS flood notification message. In the web-based manager when **Alert Notification** is selected it displays the fields to configure the notification.

Flood protection for MM1 messages prevents your subscribers from sending too many messages to your MMSC. Configuring flood protection for MM4 messages prevents another service provider from sending too many messages from the same subscriber to your MMSC.

Message flood configuration settings

The following are message flood configuration settings in **Security Profiles > Carrier > Message Flood**.

Message Flood	
Lists the large amount of messages that are being sent to you from outside sources.	
Delete	Removes messages from the list. To remove multiple messages from within the list, on the Message Flood page, in each row of the messages you want removed, select the check box and then select **Delete**. To remove all messages from the list, on the Message Flood page, select the check box in the check box column and then select **Delete**.
Remove All Entries	Removes all messages from the list.
Protocol	The protocol used.
MMS Profile	The MMS profile that is used.
Sender	The sender's email address.
Level	The level of severity of the message.
Count	The count column can be up or down and these settings can be turned off by selecting beside the column's name.
Window Size (minutes)	The time in minutes.
Timer (minutes:seconds)	The time in seconds and in minutes. The timer column can be up or down and these settings turned off by selecting beside the column's name.
Page Controls	Use to navigate through the list.

Duplicate Message

Duplicate message protection for MM1 messages prevents multiple subscribers from sending duplicate messages to your MMSC. Duplicate message protection for MM4 messages prevents another service provider from sending duplicate messages from the same subscriber to your MMSC.

The unit keeps track of the sent messages. If the same message appears more often than the threshold value that you have configured, action is taken. Possible actions are logging the duplicate messages, blocking or intercepting them, archiving, and sending an alert to inform an administrator that duplicate messages are occurring.

Duplicate message configuration settings

View duplicate messages in **Security Profiles > Carrier > Duplicate Message**.

Duplicate Message Lists duplicates of messages that were sent to you.	
Delete	Removes a message from the list. To remove multiple duplicate messages from within the list, on the Message Flood page, in each row of the messages you want removed, select the check box and then select **Delete**. To remove all duplicate messages from the list, on the Message Flood page, select the check box in the check box column and then select **Delete**.
Page Controls	Use to navigate through the list.
Remove All Entries	Removes all duplicate messages from the list.
Protocol	Either MM1 or MM4
Profile	The MMS profile that logs the detection.
Checksum	The checksum of the MMS message.
Status	Either flagged or blank. Flagged means that the actions defined in the MMS profile are taken. For more information, see "MMS bulk email filtering options".
Count	Displays the number of messages in the last window of time.
Window Size (minutes)	The period of time during which a message flood will be detected if the Message Flood Limit is exceeded.
Timer (minutes:seconds)	Either the time left in the window if the message is unflagged, or the time until the message will be unflagged if it is already flagged.

Carrier Endpoint Filter Lists

A carrier endpoint filter list contains carrier endpoint patterns. A pattern can match one carrier endpoint or can use wildcards or regular expressions to match multiple carrier endpoints. For each pattern, you select the action that the unit takes on a message when the pattern matches a carrier endpoint in the message. Actions include blocking the message, exempting the message from MMS scanning, and exempting the message from all scanning. You can also configure the pattern to intercept the message and content archive the message to a FortiAnalyzer unit.

Carrier endpoint filter lists configuration settings

The following are Carrier endpoint filter list configuration settings in **Security Profiles > Carrier > Carrier Endpoint Filter Lists**.

Carrier Endpoint Filter Lists Lists all the endpoint filters that you created. On this page, you can edit, delete or create a new endpoint filter list.	
Create New	Creates a new endpoint filter list. When you select **Create New**, you are automatically redirected to the New List page. You must enter a name to go to the Carrier Endpoint Filter Lists Settings page.
Edit	Modifies settings within an endpoint filter list in the list.
Delete	Removes an endpoint filter in the list. To remove multiple endpoint filter lists from within the list, on the Carrier Endpoint Filter List page, in each of the rows of the endpoint filter lists you want removed, select the check box and then select **Delete**. To remove all endpoint filter lists from the list, on the Carrier Endpoint Filter List page, select the check box in the check box column and then select **Delete**.
Name	The name of the endpoint filter.
# Entries	The number of carrier endpoint patterns in each carrier endpoint filter list.
MMS Profiles	The MMS profile that the carrier endpoint filter list is added to.
Comments	A description about the endpoint filter.

Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (**Security Profiles > Antivirus > Profiles**), 1 appears in **Ref.** . To view the location of the referenced object, select the number in **Ref.**, and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is avialable within the Object Usage window: • **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. • **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.

Carrier Endpoint Filter Lists Settings

Provides settings for configuring an endpoint filter.

Name	The name you entered on the New List page, after selecting **Create New** on the Carrier Endpoint Filter page.
Comments	A description about the endpoint filter. You can add one here if you did not enter one on the New List page.
Create New	Creates a new endpoint filter list. When you select **Create New**, you are automatically redirected to the New Entry page.
Edit	Select to modify the settings of a pattern in the list.
Delete	Select to remove a pattern in the list.
Enable	Enables a disabled pattern in the list.
Disable	Disables a pattern in the list.
Remove All Entries	Removes all patterns in the list on the Carrier Endpoint Filter Lists Settings page.
Enable	Indicates whether or not the pattern is enabled.

Pattern	Enter or change the pattern that FortiOS Carrier uses to match with carrier endpoints. The pattern can be a single carrier endpoint or consist of wildcards or Perl regular expressions that will match more than one carrier endpoint. Set **Pattern Type** to correspond to the pattern that you want to use.
Action	Select the action taken by FortiOS Carrier for messages from a carrier endpoint that matches the carrier endpoint pattern:
Pattern Type	The type of pattern chosen.
New Entry page	
Pattern	Enter or change the pattern that FortiOS Carrier uses to match with carrier endpoints. The pattern can be a single carrier endpoint or consist of wildcards or Perl regular expressions that will match more than one carrier endpoint. Set **Pattern Type** to correspond to the pattern that you want to use.
Action(s)	Select the action taken by FortiOS Carrier for messages from a carrier endpoint that matches the carrier endpoint pattern:
Content Archive	MMS messages from the carrier endpoint are delivered, the message content is DLP archived according to MMS DLP archive settings. Content archiving is also called DLP archiving.
Intercept	MMS messages from the carrier endpoint are delivered. Based on the quarantine configuration, attached files may be removed and quarantined.
Pattern Type	Select a pattern type as one of Single Carrier Endpoint, Wildcard or Regular Expression. Wildcard and Regular Expression will match multiple patterns where Signle Carrier Endpoint matches only one.
Enable	Select to enable this carrier endpoint filter pattern.

GTP Profile

You can configure multiple GTP profiles within the GTP menu. GTP profiles concern GTP activity flowing through the unit. These GTP profiles are then applied to a security policy.

GTP profile configuration settings

The following are GTP profile configuration settings in **Security Profiles > Carrier > GTP Profile**.

GTP Profile	
Lists each GTP profile that you have created. On this page, you can edit, delete or create a new GTP profile.	
Create New	Creates a new GTP profile. When you select **Create New**, you are automatically redirected to the New page.
Edit	Modifies settings within a GTP profile in the list. When you select **Edit**, you are automatically redirected to Edit page.
Delete	Removes a GTP profile from the list. To remove multiple GTP profiles from within the list, on the GTP Profile page, in each of the rows of the profiles you want removed, select the check box and then select **Delete**. To remove all GTP profiles from within the list, on the GTP Profile page, select the check box in the check box column and then select **Delete**.
Name	The name of the GTP profile.
Ref.	Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (**Security Profiles > Antivirus > Profiles**), 1 appears in **Ref.** . To view the location of the referenced object, select the number in **Ref.**, and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is avialable within the Object Usage window: • **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. • **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page. • **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy's settings appear within the table.
New GTP Profile	
Provides settings for configuring a GTP profile.	

Name	Enter a name for the GTP profile.
General Settings	Configure general options for the GTP profile..
Message Type Filtering	Configure filtering for messages.
APN Filtering	Configure filtering options for APN.
IMSI Filtering	Configure filtering options for IMSI.
Advanced Filtering	Configure advanced filtering options.
IE removal policy	Configure IE removal policy options.
Encapsulated IP Traffic Filtering	Configure filtering options for encapsulated IP traffic.
Encapsulated Non-IP End User Address Filtering	Configure filtering options for encapsulated non-IP end user addresses.
Protocol Anomaly	Configure protocol anomaly options.
Anti-Overbilling	Configure anti-overbilling options.
Log	Configure log options.

General settings options

The following are mostly house keeping options that appear in the General Settings area of the GTP configuration page.

General Settings section of the New GTP Profile	
Sequence Number Validation	Enable to check that packets are not duplicated or out of order. GTP packets contain a Sequence Number field. This number tells the receiving GGSN the order of the packets it is receiving. Normally the GGSN compares this sequence number in the packets with its own sequence counter — if the two do not match, the packet is dropped. This sequence number validation can be off-loaded to the FortiOS Carrier freeing up resources on the GGSN.
GTP-in-GTP	Select **Allow** to enable GTP packets to be allowed to contain GTP packets, or a GTP tunnel inside another GTP tunnel. To block all GTP-in-GTP packets, select **Deny**.
Minimum Message Length	Enter the shortest possible message length in bytes. Normally this is controlled by the protocol, and will vary for different message types. If a packet is smaller than this limit, it is discarded as it is likely malformed and a potential security risk. The default minimum message length is 0 bytes.
Maximum Message Length	Enter the maximum allowed length of a GTP packet in bytes. A GTP packet contains three headers and corresponding parts GTP, UDP, and IP. If a packet is larger than the maximum transmission unit (MTU) size, it is fragmented to be delivered in multiple packets. This is inefficient, resource intensive, and may cause problems with some applications. By default the maximum message length is 1452 bytes.
Tunnel Limit	Enter the maximum number of tunnels allowed open at one time. For additional GTP tunnels to be opened, existing tunnels must first be closed. This feature can help prevent a form of denial of service attack on your network. This attack involves opening more tunnels than the network can handle and consuming all the network resources doing so. By limiting the number of tunnels at any one time, this form of attack will be avoided. The tunnel limiting applies to the Handover Group, and Authorized SGSNs and GGSNs.
Tunnel Timeout	Enter the maximum number of seconds that a GTP tunnel is allowed to remain active. After this hard timeout, the unit deletes the GTP tunnel. A GTP tunnel may hang for various reasons. For example, during the GTP tunnel tear-down stage, the "delete pdap context response" message may get lost. By setting a timeout value, you can configure the FortiOS Carrier firewall to remove the hanging tunnels. The default is 86400 seconds, or 24 hours.

General Settings section of the New GTP Profile	
Control plane message rate limit	Enter the number of packets per second to limit the traffic rate to protect the GSNs from possible Denial of Service (DoS) attacks. The default limit of **0** does not limit the message rate. GTP DoS attacks can include: • **Border gateway bandwidth saturation**: A malicious operator can connect to your GRX and generate high traffic towards your Border Gateway to consume all the bandwidth. • **GTP flood**: A GSN can be flooded by illegitimate traffic
Handover Group	Select the allowed list of IP addresses allowed to take over a GTP session when the mobile device moves locations. Handover is a fundamental feature of GPRS/UMTS, which enables subscribers to seamlessly move from one area of coverage to another with no interruption of active sessions. Session hijacking can come from the SGSN or the GGSN, where a fraudulent GSN can intercept another GSN and redirect traffic to it. This can be exploited to hijack GTP tunnels or cause a denial of service. When the handover group is defined it acts like a whitelist with an implicit default deny at the end — the GTP address must be in the group or the GTP message will be blocked. This stops handover requests from untrusted GSNs.
Authorized SGSNs	Use **Authorized SGSNs** to only allow authorized SGSNs to send packets through the unit and to block unauthorized SGSNs. Go to **Firewall Objects > Address > Addresses** and add the IP addresses of the authorized SGSNs to a firewall address or address group. Then set **Authorized SGSNs** to this firewall address or address group. You can use **Authorized SGSNs** to allow packets from SGSNs that have a roaming agreement with your organization.
Authorized GGSNs	Use **Authorized GGSNs** to only allow authorized GGSNs to send packets through the unit and to block unauthorized GGSNs. Go to **Firewall Objects > Address > Addresses** and add the IP addresses of the authorized GGSNs to a firewall address or address group. Then set **Authorized GGSNs** to this firewall address or address group. You can use Authorized GGSNs to allow packets from SGSNs that have a roaming agreement with your organization.

Message type filtering options

On the **New GTP Profile** page, you can select to allow or deny the different types of GTP messages, which is referred to as message type filtering. You must expand the Message Type Filtering section to access the

settings.

The messages types include Path Management, Tunnel Management, Location Management, Mobility Management, MBMS, and GTP-U and Charging Management messages.

For enhanced security, Fortinet best practices dictate that you set Unknown Message Action to deny. This will block all unknown GTP message types, some of which may be malicious.

To configure message type filter options, expand **Message Type Filtering** in the GTP profile.

APN filtering options

An Access Point Name (APN) is an Information Element (IE) included in the header of a GTP packet. It provides information on how to reach a network.

An APN has the following format:

```
<network_id>[.mnc<mnc_int>.mcc<mcc_int>.gprs]
```

Where:

- `<network_id>` is a network identifier or name that identifies the name of a network, for example, `example.com` or `internet`.
- `[.mnc<mnc_int>.mcc<mcc_int>.gprs]` is the optional operator identifier that uniquely identifies the operator's PLMN, for example `mnc123.mcc456.gprs`.

Combining these two examples results in a complete APN of `internet.mnc123.mcc456.gprs`.

By default, the unit permits all APNs. However, you can configure APN filtering to restrict roaming subscribers' access to external networks.

APN filtering applies only to the GTP **create pdp request** messages. The unit inspects GTP packets for both APN and selected modes. If both parameters match and APN filter entry, the unit applies the filter to the traffic.

Additionally, the unit can filter GTP packets based on the combination of an IMSI prefix and an APN.

You cannot add an APN when creating a new profile.

APN Filtering	
Enable APN Filter	Select to enable APN filtering.
Default APN Action	Select the default action for APN filtering. If you select **Allow**, all sessions are allowed except those blocked by individual APN filters. If you select **Deny**, all sessions are blocked except those allowed by individual APN filters.
Value	The APN to be filtered.
Mode	The type of mode chosen that indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription:
Action	The type of action that will be taken.
Edit	Modifies the settings within the filter. When you select **Edit**, the Edit window appears, which allows you to modify the settings of the APN.
Delete	Removes the APN from the list within the table, in the APN Filtering section.
Add APN	Adds a new APN filter to the list. When you select **Add APN**, the New window appears, which allows you to configure the APN settings.
New APN page	
Value	Enter an APN to be filtered. You can include wild cards to match multiple APNs. For example, the value **internet*** would match all APNs that being with **internet**.
Mode	Select one or more of the available modes to indicate where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.
Mobile Station provided	MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network.
Network provided	Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network.
Subscription Verified	MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network
Action	Select **Allow** or **Deny**.

Basic filtering options

The International Mobile Station Identity (IMSI) is used by a GPRS Support Node (GSN) to identify a mobile station. Three elements make up every IMSI:

- the mobile country code (MCC)
- the mobile network code (MNC)
- the mobile subscriber identification number (MSIN).

The subscriber's home network—the public land mobile network (PLMN)—is identified by the IMSI prefix, formed by combining the MCC and MNC.

By default, the unit allows all IMSIs. You can add IMSI prefixes to deny GTP traffic coming from non-roaming partners. Any GTP packets with IMSI prefixes not matching the prefixes you set will be dropped. GTP **Create pdp** request messages are filtered and only IMSI prefixes matching the ones you set are permitted. Each GTP profile can have up to 1000 IMSI prefixes set.

An IMSI prefix and an APN can be used together to filter GTP packets if you set an IMSI filter entry with a non-empty APN.

You cannot add an IMSI when creating a new profile. You must add it after the profile has been created and you are editing the profile.

IMSI Filtering section of the New GTP Profile	
Enable IMSI Filter	Select to enable IMSI filtering.
Default IMSI Action	Select the default action for IMSI filtering. If you select **Allow**, all sessions are allowed except those blocked by individual IMSI filters. If you select **Deny**, all sessions are blocked except those allowed by individual IMSI filters.
APN	The APN that is part of the IMSI that will be filtered.
MCC-MNC	The MCC-MNC part of the IMSI that will be filtered.
Mode	The type of mode that indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.
Action	The type of action that will be taken.
Edit	Modifies settings to an IMSI filter. When you select **Edit**, the Edit window appears, which allows you to modify the IMSI filter's settings.
Delete	Removes an IMSI filter from within the table, in the IMSI Filtering section.
Add IMSI	Adds a new IMSI filter to the list. When you select **Add IMSI**, the New window appears, which allows you to configure IMSI filter settings.
New IMSI page	
APN	Enter the APN part of the IMSI to be filtered.
MCC-MNC	Enter the MCC-MCC part of the IMSI to be filtered.
Mode	Select one or more of the available modes to indicate where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.
Mobile Station provided	MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network.
Network provided	Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network.
Subscription Verified	MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network
Action	Select **Allow** or **Deny**.

Advanced filtering options

The FortiOS Carrier firewall supports advanced filtering against the attributes RAT, RAI, ULI, APN restriction, and IMEI-SV in GTP to block specific harmful GPRS traffic and GPRS roaming traffic. The following table shows some of the GTP context requests and responses that the firewall supports.

Attributes supported by FortiCarrier firewalls

	GTP Create PDP Context Request	GTP Create PDP Context Response	GTP Update PDP Context Request	GTP Update PDP Context Response
APN	yes	yes	-	
APN Restriction	yes	-	-	yes
IMEI-SV	yes	-	-	-
IMSI	yes	-	yes	-
RAI	yes	-	yes	-
RAT	yes	-	yes	-
ULI	yes	-	yes	-

When editing a GTP profile, select **Advanced Filtering > Add** to create and add a rule. When the rule matches traffic it will either allow or deny that traffic as selected in the rule.

Advanced Filtering	
Enable	Select to enable advanced filtering.
Default Action	Select the default action for advanced filtering. If you select **Allow**, all sessions are allowed except those blocked by individual advanced filters. If you select **Deny**, all sessions are blocked except those allowed by individual advanced filters.
Messages	The messages, for example, Create PDP Context Request.
APN Restriction	The APN restriction.
RAT Type	The RAT types associated with that filter.
ULI	The ULI pattern.
RAI	The RAI pattern.
IMEI	The IMEI pattern.
Action	The action that will be taken.
Edit	Modifies the filter's settings. When you select **Edit**, the Edit window appears, which allows you to modify the filter's settings.
Delete	Removes a filter from the list.
Add	Adds a filter to the list. When you select **Add**, the New window appears, which allows you to configure settings for messages, APN, IMSI, MSISDN, RAT type, ULI, RAI, IMEI patterns as well as the type of action.
New Filtering page	
Messages	The PDP content messages this profile will match.
Create PDP Context Request	Select to allow create PDP context requests.
Create PDP Context Response	Select to allow create PDP context responses.
Update PDP Context Request	Select to allow update PDP context requests.
Update PDP Context Response	Select to allow update PDP context responses.

APN	Enter the APN.
APN Mode	Select an APN mode as one or more of • Mobile Station provied • Network provided • Subscription provied This field is only available when an APN has been entered.
Mobile Station provided	MS-provided PAN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network.
Network provided	Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR did no verify the user's subscription to the network.
Subscription verified	MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.
APN Restriction	Select the type of restriction that you want. You can choose all of the types, or one of the types. You cannot choose multiple types. Types include: • all • Public-1 • Public-2 • Private-1 • Private-2
IMSI	Enter the IMSI.
MSISDN	Enter the MSISDN.
RAT Type	Optionally select the RAT type as any combination of the following: • Any • UTRAN • GERAN • Wifi • GAN • HSPA Some RAT types are GTPv1 specific.
ULI pattern	Enter the ULI pattern.
RAI pattern	Enter the RAI pattern.

IMEI pattern	Enter the IMEI pattern.
Action	Select either **Allow** or **Deny**.

Adding an advanced filtering rule

When adding a rule, use the following formats:

- Prefix, for example, range 31* for MCC matches MCC from 310 to 319.
- Range, for example, range 310-319 for MCC matches MCC from 310 to 319.
- Mobile Country Code (MCC) consists of three digits. The MCC identifies the country of domicile of the mobile subscriber.
- Mobile Network Code (MNC) consists of two or three digits for GSM/UMTS applications. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. Best practices dictate not to mix two and three digit MNC codes within a single MCC area.
- Location Area Code (LAC) is a fixed length code (of 2 octets) identifying a location area within a PLMN. This part of the location area identification can be coded using a full hexadecimal representation except for the following reserved hexadecimal values: 0000 and FFFE. These reserved values are used in some special cases when no valid LAI exists in the MS (see 3GPP TS 24.008, 3GPP TS 31.102 and 3GPP TS 51.011).
- Routing Area Code (RAC) of a fixed length code (of 1 octet) identifies a routing area within a location.
- CI or SAC of a fixed length of 2 octets can be coded using a full hexadecimal expression.
- Type Allocation Code (TAC) has a length of 8 digits.
- Serial Number (SNR) is an individual serial number identifying each equipment within each TAC. SNR has a length of 6 digits.
- Software Version Number (SVN) identifies the software version number of the mobile equipment. SVN has a length of 2 digits.

You cannot add an advanced filtering rule when creating a new profile. You must add it after the profile has been created and you are editing the profile.

Information Element (IE) removal policy options

In some roaming scenarios, the unit is installed on the border of the PLMN and the GRX. In this configuration, the unit supports information element (IE) removal policies to remove any combination of R6 IEs (RAT, RAI, ULI, IMEI-SV and APN restrictions) from the types of messages described in "Advanced filtering options", prior to forwarding the messages to the HGGSN (proxy mode).

IE removal policy	
Enable	Select to enable this option.
SGSN address of message IE	The firewall address or address group that contains the SGSN addresses.
IEs to be removed	The IE types that will be removed. These include APN Restriction, RAT, RAI, ULI, and IMEI.
Add	Adds an IE removal policy. When you select **Add**, the New window appears, which allows you to configure the IE policy.
Edit	Modifies settings from within the IE removal policy. When you select **Edit**, the Edit window appears, which allows you to modify the settings within the policy.
Delete	Removes the IE removal policy from the list.
New IE policy page	
SGSN address	Select a firewall address or address group that contains SGSN addresses.
IEs to be removed	Select one or more IE types to be removed. These include APN Restriction, RAT, RAI, ULI, and IMEI.

Encapsulated IP traffic filtering options

You can use encapsulated IP traffic filtering to filter GTP sessions based on information contained in the data stream. to control data flows within your infrastructure. You can configure IP filtering rules to filter encapsulated IP traffic from mobile stations by identifying the source and destination policies. For more information, see When to use encapsulated IP traffic filtering.

Expand **Encapsulated IP Traffic Filtering** in the GTP profile to reveal the options.

Encapsulated IP Traffic Filtering	
Enable IP Filter	Select to enable encapsulated IP traffic filtering options.
Default IP Action	Select the default action for encapsulated IP traffic filtering. If you select **Allow**, all sessions are allowed except those blocked by individual encapsulated IP traffic filters. If you select **Deny**, all sessions are blocked except those allowed by individual encapsulated IP traffic filters.
Source	Select a source IP address from the configured firewall IP address or address group lists. Any encapsulated traffic originating from this IP address will be a match if the destination also matches.
Destination	Select a destination IP address from the configured firewall IP address or address group lists. Any encapsulated traffic being sent to this IP address will be a match if the destination also matches.
Action	The type of action that will be taken. Select to **Allow** or **Deny** encapsulated traffic between this source and Destination.
Edit	Modifies the source, destination or action settings.
Add IP Policy	Adds a new encapsulated IP traffic filter. When you select **Add IP Policy**, the New window appears which allows you to configure IP policy settings.
New (window)	
Source	Select the source firewall address or address group.
Destination	Select the destination firewall address or address group.
Action	Select **Allow** or **Deny**.

Encapsulated non-IP end user traffic filtering options

Depending on the installed environment, it may be beneficial to detect GTP packets that encapsulate non-IP based protocols. You can configure the FortiOS Carrier firewall to permit a list of acceptable protocols, with all other protocols denied.

The encoded protocol is determined in the PDP Type Organization and PDP Type Number fields within the End User Address Information Element. The PDP Type Organization is a 4-bit field that determines if the protocol is part of the ETSI or IETF organizations. Values are zero and one, respectively. The PDP Type field is one byte long. Both GTP specifications list only PPP, with a PDP Type value of one, as a valid ETSI protocol. PDP Types for the IETF values are determined in the “Assigned PPP DLL Protocol Numbers” sections of RFC1700. The PDP types are compressed, meaning that the most significant byte is skipped, limiting the protocols listed from 0x00 to 0xFF.

Encapsulated Non-IP End User Address Filtering	
Enable Non-IP Filter	Select to enable encapsulated non-IP traffic filtering.
Default Non-IP Action	Select the default action for encapsulated non-IP traffic filtering. If you select **Allow**, all sessions are allowed except those blocked by individual encapsulated non-IP traffic filters. If you select **Deny**, all sessions are blocked except those allowed by individual encapsulated non-IP traffic filters.
Type	The type chosen, **AESTI** or **IETF.**
Start Protocol	The beginning protocol port number range.
End Protocol	The end of the protocol port number range.
Action	The type of action that will be taken.
Edit	Modify a non-IP filter's settings in the list. When you select **Edit**, the Edit window appears, which allows you to modify the Non-IP policy settings.
Delete	Remove a non-IP policy from the list.
Add Non-IP Policy	Add a new encapsulated non-IP traffic filter. When you select **Add Non-IP Policy**, you are automatically redirected to the New page.
New (window)	
Type	Select **AESTI** or **IETF**.
Start Protocol **End Protocol**	Select a start and end protocol from the list of protocols in RFC 1700. Allowed range includes 0 to 255 (0x00 to 0xff). Some common protocols include: • 33 (0x0021) Internet Protocol • 35 (0x0023) OSI Network Layer • 63 (0x003f) NETBIOS Framing • 65 (0x0041) Cisco Systems • 79 (0x004f) IP6 Header Compression • 83 (0x0053) Encryption
Action	Select **Allow** or **Deny**.

Protocol Anomaly prevention options

Use protocol anomaly detection options to detect or deny protocol anomalies according to GTP standards and tunnel state. Protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of the protocol specifications. Packets cannot pass through if they fail the sanity check.

Protocol Anomaly	
Invalid Reserved Field	GTP version 0 (GSM 09.60) headers specify a number of fields that are marked as "Spare" and contain all ones (1). GTP packets that have different values in these fields are flagged as anomalies. GTP version 1 (GSM 29.060) makes better use of the header space and only has one, 1-bit, reserved field. In the first octet of the GTP version1 header, bit 4 is set to zero.
Reserved IE	Both versions of GTP allow up to 255 different Information Elements (IE). However, a number of Information Elements values are undefined or reserved. Packets with reserved or undefined values will be filtered.
Miss Mandatory IE	GTP packets with missing mandatory Information Elements (IE) will not be passed to the GGSN.
Out of State Message	The GTP protocol requires a certain level of state to be kept by both the GGSN and SGSN. Some message types can only be sent when in a specific GTP state. Packets that do not make sense in the current state are filtered or rejected Both versions of GTP allow up to 255 different message types. However, a number of message type values are undefined or reserved. Best practices dictate that packets with reserved or undefined values will be filtered.
Out of State IE	GTP Packets with out of order Information Elements are discarded.
Spoofed Source Address	The End User Address Information Element in the PDP Context Create & Response messages contain the address that the mobile station (MS) will use on the remote network. If the MS does not have an address, the SGSN will set the End User Address field to zero when sending the initial PDP Context Create message. The PDP Context Response packet from the GGSN will then contain an address to be assigned to the MS. In environments where static addresses are allowed, the MS will relay its address to the SGSN, which will include the address in the PDP Context Create Message. As the MS address is negotiated within the PDP Context creation handshake, any packets originating from the MS that contain a different source address are detected and dropped.

Anti-Overbilling options

You can configure the FortiOS Carrier firewall to prevent overbilling subscribers for traffic over the. To enable anti-overbilling, you must configure both the Gn/Gp firewall and the Gi firewall.

Expand **Anti-Overbilling** in the GTP profile to reveal these settings.

Anti-Overbilling	
Gi Firewall IP Address	The IP address of the unit's interface configured as a Gi gateway.
Port	The SG security port number. The default port number is port 21123. Change this number if your system uses a different SG port.
Interface	Select the unit interface configured as a Gi gateway.
Security Context ID	Enter the security context ID. This ID must match the ID entered on the server Gi firewall. The default security context ID is 696.

Log options

All the GTP logs are treated as a subtype of the event logs. To enable GTP logging, you must:

- configure the GTP log settings in a GTP profile
- enable GTP logging when you configure log and report settings.

To enable GTP logging after a GTP profile has been configured

1. Go to **Log & Report > Log Config > Log Settings**.
2. Select **Event Logging**, and select **GTP service event**.
3. Select **Apply**.

Log	
Log Frequency	Enter the number of messages to drop between logged messages. An overflow of log messages can sometimes occur when logging rate-limited GTP packets exceed their defined threshold. To conserve resources on the syslog server and the Carrier-enabled FortiGate unit, you can specify that some log messages are dropped. For example, if you want only every twentieth message to be logged, set a logging frequency of 20. This way, 20 messages are skipped and the next logged. Acceptable frequency values range from 0 to 2147483674. When set to '0', no messages are skipped.
Forwarded Log	Select to log forwarded GTP packets.
Denied Log	Select to log GTP packets denied or blocked by this GTP profile.
Rate Limited Log	Select to log rate-limited GTP packets.
State Invalid Log	Select to log GTP packets that have failed stateful inspection.
Tunnel Limit Log	Select to log packets dropped because the maximum limit of GTP tunnels for the destination GSN is reached.

Extension Log	Select to log extended information about GTP packets. When enabled, this additional information will be included in log entries: • IMSI • MSISDN • APN • Selection Mode • SGSN address for signaling • SGSN address for user data • GGSN address for signaling • GGSN address for user data
Traffic count Log	Select to log the total number of control and user data messages received from and forwarded to the GGSNs and SGSNs that the unit protects. The unit can report the total number of user data and control messages received from and forwarded to the GGSNs and SGSNs it protects. Alternately, the total size of the user data and control messages can be reported in bytes. The unit differentiates between traffic carried by each GTP tunnel, and also between GTP-User and GTP-Control messages. The number of messages or the number of bytes of data received from and forwarded to the SGSN or GGSN are totaled and logged if a tunnel is deleted. When a tunnel is deleted, the log entry contains: • Timestamp • Interface name (if applicable) • SGSN IP address • GGSN IP address • TID • Tunnel duration time in seconds • Number of messages sent to the SGSN • Number of messages sent to the GGSN

Specifying logging types

You can configure the unit to log GTP packets based on their status with GTP traffic logging.

The status of a GTP packet can be any of the following 5 states:

- **Forwarded** - a packet that the unit transmits because the GTP policy allows it
- **Prohibited** - a packet that the unit drops because the GTP policy denies it
- **Rate-limited** - a packet that the unit drops because it exceeds the maximum rate limit of the destination GSN
- **State-invalid** - a packet that the unit drops because it failed stateful inspection
- **Tunnel-limited** - a packet that the unit drops because the maximum limit of GTP tunnels for the destination GSN is reached.

The following information is contained in each log entry:

- Timestamp
- Source IP address

- Destination IP address
- Tunnel Identifier (TID) or Tunnel Endpoint Identifier (TEID)
- Message type
- Packet status: forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited
- Virtual domain ID or name
- Reason to be denied if applicable.

MMS Security features

FortiOS Carrier includes all the Security features of FortiOS with extra features specific to MMS carrier networks.

This section includes:

Why scan MMS messages for viruses and malware?
MMS virus scanning
Sender notifications and logging
MMS content-based Antispam protection
MMS DLP archiving

Why scan MMS messages for viruses and malware?

The requirement for scanning MM1 content comes from the fact that MMS is an increasingly popular technique for propagating malware between mobile devices.

Example: COMMWARRIOR

This is a virus for Series 60 type cell phones, such as Nokia, operating Symbian OS version 6 [or higher]. The object of the virus is to spread to other phones using Bluetooth and MMS as transport avenues. The targets are selected from the contact list of the infected phone and also sought via Bluetooth searching for other Bluetooth-enabled devices (phones, printers, gaming devices etc.) in the proximity of the infected phone.

This virus is more than a proof of concept - it has proven successfully its ability to migrate from a zoo collection to being in-the-wild. Currently, this virus is being reported in over 18 different countries around Europe, Asia and North America.

When the virus first infects a cell phone, a prompt is displayed asking the recipient if they want to install “Caribe”. Symptoms of an infected phone may include rapid battery power loss due to constant efforts by the virus to spread to other phones via a Bluetooth seek-and-connect outreach.

The following variants among others are currently scanned by the FortiOS Carrier devices, in addition to more signatures that cover all known threats.

- **SymbOS/COMWAR.V10B!WORM**
- Aliases: SymbOS.Commwarrior.B, SymbOS/Commwar.B, SymbOS/Commwar.B!wm, SymbOS/Commwar.B-net, SymbOS/Commwarrior.b!sis, SymbOS/Comwar.B, SymbOS/Comwar.B!wm, SymbOS/Comwar.B-wm, SYMBOS_COMWAR.B, SymbOS/Comwar.1.0.B!wormSYMBOS/COMWAR.V10B.SP!WORM [spanish version]
- First Discovered In The Wild: July 04, 2007
- Impact Level: 1
- Virus Class: Worm
- Virus Name Size: 23,320
- **SymbOS/Commwar.A!worm**
- Aliases: Commwarrior-A, SymbOS.Commwarrior.A [NAV], SymbOS/Commwar.A-net, SymbOS/Commwar_ezboot.A-ne, SymbOS/Comwar.A, SymbOS/Comwar.A-wm, SYMBOS_COMWAR.A [Trend]
- First Discovered In The Wild: May 16 2005
- Impact Level: 1

- Virus Class: Worm
- Virus Name Size: 27,936
- SymbOS/Commwarriie.C-wm
- Aliases: None
- First Discovered In The Wild: Oct 17 2005
- Impact Level: 1
- Virus Class: File Virus
- Virus Name Size: None

For the latest list of threats Fortinet devices detect, visit the FortiGuard Center.

MMS virus scanning

You can use MMS virus scanning to scan content contained within MMS messages for viruses. FortiOS Carrier virus scanning can be applied to the MM1, MM3, MM4, and MM7 interfaces to detect and remove content containing viruses at many points in an MMS network. Perhaps the most useful interface to apply virus scanning would be the MM1 interface to block viruses sent by mobile users before they get into the service provider network.

To go to MMS virus scanning, go to **Security Profiles > Carrier > MMS Profile**, select an existing or create a new profile, and expand **MMS Scanning**. See MMS scanning options.

This section includes:

- MMS virus monitoring
- MMS virus scanning blocks messages (not just attachments)
- Scanning MM1 retrieval messages
- Configuring MMS virus scanning
- Removing or replacing blocked messages
- Carrier Endpoint Block
- MMS Content Checksum
- Passing or blocking fragmented messages
- Client comforting
- Server comforting
- Handling oversized MMS messages

MMS virus monitoring

To enable MMS virus monitoring, expand **MMS Scanning** and enable **Monitor only** for the selected MMS types.

This feature causes the FortiOS Carrier unit to record log messages when MMS scanning options find a virus, match a file name, or match content using any of the other MMS scanning options. Selecting this option enables reporting on viruses and other problems in MMS traffic without affecting users.

MMS virus scanning blocks messages (not just attachments)

To enable MMS virus scanning, expand **MMS Scanning** and enable **Virus Scan** for the selected MMS types.

Because MM1 and MM7 use HTTP, the oversize limits for HTTP and the HTTP antivirus port configurations also apply to MM1 and MM7 scanning. See

MM3 and MM4 use SMTP and the oversize limits for SMTP and the SMTP antivirus port configurations also apply to MM3 and MM4 scanning.

The message contents will be scanned for viruses, matched against the file extension blocking lists and scanned for banned words. All these items will be configured via the standard GUI interfaces available for the other protocols and will be controlled at the protection profile level with new options specifically for the MM1 messages.

The FortiOS Carrier unit extracts the sender's Mobile Subscriber Integrated Services Digital Network Number (MSISDN) from the HTTP headers if available. The `POST` payload will be sent to the scanunits which will parse the MMS content and scan each message data section. If any part of the data is to be blocked, the proxy will be informed, the connection to the MMSC will be reset and the Carrier-enabled FortiGate unit will return an `HTTP 200 OK` message with an `m-send-conf` payload to the client to prevent a retry. Finally the appropriate logging, alert, and replacement message events will be triggered.

For client notification, the `x-mms-response-status` and `x-mms-response-text` fields can also be customized as required.

Scanning MM1 retrieval messages

To scan MM1 retrieval messages, expand **MMS Scanning** and select **Scan MM1 message retrieval**.

Select to scan message retrievals that use MM1. If you enable **Virus Scan** for all MMS interfaces, messages are also scanned while being sent. In this case, you can disable MM1 message retrieval scanning to improve performance.

Configuring MMS virus scanning

To configure MMS virus scanning, expand **MMS Scanning** and enable **Virus Scan**.

Once applied to a security policy, the MMS protection profile will then perform virus scans on all traffic accepted by that policy.

Removing or replacing blocked messages

To remove blocked messages, expand **MMS Scanning** and select **Remove Blocked** for the selected MMS types.

Select **Remove Blocked** remove blocked content from each protocol and replace it with the replacement message. If FortiOS Carrier is to preserve the length of the message when removing blocked content, as may occur when billing is affected by the length of the message, select **Constant**.

If you only want to monitor blocked content, select **Monitor Only**.

Carrier Endpoint Block

A carrier endpoint defines a specific client on the carrier network. Typically the client IP address is used to identify the client, however on a carrier network this may be impractical when the client is using a mobile device. Other identifying information such as the MSIDSN number is used instead.

This information can be used to block a specific endpoint on the network. Reasons for blocking may include clients whose accounts have expired, clients from another carrier, clients who have sent malicious content (phishing, exploits, viruses, etc), or other violations of terms of use.

Enabling carrier endpoint blocking

To enable carrier endpoint blocking you first need to create a carrier endpoint filter list, and then enable it.

To enable carrier endpoint blocking - web-based manager

1. Create a carrier endpoint filter list.
2. Go to **Security Profiles > Carrier > MMS Profile**.
3. Select **Create New**, or select an existing profile to edit and select **Edit**.
4. Expand MMS Scanning.
5. Select one or more types of MMS messaging to enable endpoint blocking on.
6. Select the carrier endpoint filter list to use in matching the endpoints to be blocked.

In MMS Profile, endpoints can only be blocked.

Create a carrier endpoint filter list

A carrier endpoint filter list contains one or more carrier endpoints to match. When used in MMS scanning entries in the filter list that are matched are blocked.

You can configure multiple filter lists for different purposes and groups of clients, such as blocking clients, clients with different levels of service agreements, and clients from other carriers. See Carrier endpoint filter lists configuration settings.

To create a carrier endpoint filter list - web-based manager

1. Go to **Security Profiles > Carrier > Carrier Endpoint Filter Lists**.
2. Select **Create New**.
3. Enter a descriptive name for the filter list, such as `blocked_clients` or `CountryX_clients`, and select **OK**.
4. Select **Create New** to add one or more entries to the list.
5. Select **OK** to return to display the list of filter lists.

Configuring endpoint filter list entries

For each single endpoint or group of endpoints have part of their identifying information in common, you create an entry in the endpoint filter list.

For example a `blocked_clients` filter list may include entries for single endpoints added as each one needs to be blocked and a group of clients from a country that does not allow certain services.

To configure an endpoint filter list entry - web-based manager

1. Select **Create New**.
2. Enter the following information and select **OK**.

Name	Name of endpoint filter list. Select this name in an MMS protection profile.
Comments	Optional description of the endpoint filter list.
Check/Uncheck All	Select the check box to enable all endpoint patterns in the MMS filter list. Clear the check box to disable all entries on the MMS filter list. You can also select or clear individual check boxes to enable or disable individual endpoint patterns.
Pattern	The pattern that FortiOS Carrier uses to match with endpoints. The pattern can be a single endpoint or consist of wildcards or Perl regular expressions that will match more than one endpoint. For more on wildcard and regular expressions, see Using wildcards and Perl regular expressions in the UTM guide.
Action	Select the action taken by FortiOS Carrier for messages from a carrier endpoint that matches the endpoint pattern: **None** - No action is taken. **Block** - MMS messages from the endpoint are not delivered and FortiOS Carrier records a log message. **Exempt from mass MMS** - MMS messages from the endpoint are delivered and are exempt from mass MMS filtering. Mass MMS filtering is configured in MMS protection profiles and is also called MMS Bulk Email Filtering and includes MMS message flood protection and MMS duplicate message detection. A valid use of mass MMS would be when a service provider notifies customers of a system-wide event such as a shutdown. **Exempt from all scanning** - MMS messages from the endpoint are delivered and are exempt from all MMS protection profile scanning.
Content Archive	MMS messages from the endpoint are delivered, the message content is DLP archived according to MMS DLP archive settings. Content archiving is also called DLP archiving.
Intercept	MMS messages from the endpoint are delivered. Based on the quarantine configuration, attached files may be removed and quarantined.
Pattern Type	The pattern type: **Wildcard**, **Regular Expression**, or **Single Endpoint**.
Enable	Select to enable this endpoint filter pattern.

Blocking network access based on endpoints

You can use endpoint IP filtering to block traffic from source IP addresses associated with endpoints. You can also configure FortiOS Carrier to record log messages whenever endpoint IP filtering blocks traffic. Endpoint IP filtering blocks traffic at the IP level, before the traffic is accepted by a security policy.

To configure endpoint IP filtering, go to **Security Profiles > Carrier > IP Filter** and add endpoints to the IP filter list. For each endpoint you can enable or disable both blocking traffic and logging blocked traffic.

You cannot add endpoint patterns to the endpoint IP filter list. You must enter complete and specific endpoints that are valid for your network.

The only action available is block. You cannot use endpoint IP filtering to exempt endpoints from IP filtering or to content archive or quarantine communication sessions.

FortiOS Carrier looks in the current user context list for the endpoints in the IP filter list and extracts the source IP addresses for these endpoints. Then any communication session with a source IP address that matches one of these IP addresses is blocked at the IP level, before the communication session is accepted by a security policy.

FortiOS Carrier dynamically updates the list of IP addresses to block as the user context list changes. Only these updated IP addresses are blocked by endpoint IP filtering.

For information about the carrier endpoints and the user context list, including how entries are added to and removed from this list.

MMS Content Checksum

The MMS content checksum feature attempts to match checksums of known malicious MMS messages, and on a successful match it will be blocked. The checksums are applied to each part of the message—attached files and message body have separate checksums. These checksums are created with CRC-32, the same method as FortiAnalyzer checksums.

For example, if an MMS message contains a browser exploit in the message body, you can add the checksum for that message body to the list, and future occurrences of that exact message will be blocked. Content will be replaced by the content checksum block notification replacement message for that type of MMS message, and if it is enabled the event will be logged.

One possible implementation would to configure all .sis files to be intercepted. When one is found to be infected or malicious it would be added to the MMS content checksum list.

To use this feature a list of one or more malicious checksums must be created and then the feature is enabled using that list. For a detailed list of options, see MMS Content Checksum.

To configure an MMS content checksum list

1. Go to **Security Profiles > Carrier > MMS Content Checksum**.
2. Select **Create New**.
3. Enter a name for the list of checksums, and select **OK**.
   You are taken to the edit screen for that new list.

4. Select ***Create New*** to add a checksum.
5. Enter the ***Name*** and ***Checksum***, and select **OK**.
   The checksum is added to the list.

To add more checksums to the list, repeat steps 4 and 5.

To to remove a checksum from the list you can either delete the checksum or simply disable it and leave it in the list.

To enable MMS content checksums, expand **MMS Scanning** and select **MMS Content Checksum** for the selected MMS types. Select the checksum list to match.

Passing or blocking fragmented messages

Select to pass fragmented MM3 and MM4 messages. Fragmented MMS messages cannot be scanned for viruses. If you do not select these options, fragmented MM3 and MM4 message are blocked.

The Interval is the time in seconds before client comforting starts after the download has begun, and the time between sending subsequent data.

The **Amount** is the number of bytes sent by client or server comforting at each interval.

Client comforting

In general, client comforting is available for for MM1 and MM7 messaging and provides a visual display of progress for web page loading or HTTP or FTP file downloads. Client comforting does this by sending the first few packets of the file or web page being downloaded to the client at configured time intervals so that the client is not aware that the download has been delayed. The client is the web browser or FTP client. Without client comforting, clients and their users have no indication that the download has started until the Carrier-enabled FortiGate unit has completely buffered and scanned the download. During this delay users may cancel or repeatedly retry the transfer, thinking it has failed.

The appearance of a client comforting message (for example, a progress bar) is client-dependent. In some instances, there will be no visual client comforting cue.

During client comforting, if the file being downloaded is found to be infected, then the Carrier-enabled FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead the download stops, and the user is left with a partially downloaded file.

If the user tries to download the same file again within a short period of time, then the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.

Client comforting can send unscanned (and therefore potentially infected) content to the client. Only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

MM1 and MM7 client comforting steps

Since MM1 and MM7 messages use HTTP, MM1 and MM7 client comforting operates like HTTP client comforting.

The following steps show how client comforting works for a download of a 1 Mbyte file with the client comforting interval set to 20 seconds and the client comforting amount set to 512 bytes.

1. The client requests the file.
2. The Carrier-enabled FortiGate unit buffers the file from the server. The connection is slow, so after 20 seconds about one half of the file has been buffered.
3. The Carrier-enabled FortiGate unit continues buffering the file from the server, and also sends 512 bytes to the client.
4. After 20 more seconds, the FortiGate unit sends the next 512 bytes of the buffered file to the client.
5. When the file has been completely buffered, the client has received the following amount of data:

   ```
   ca * (T/ci) bytes == 512 * (40/20) == 512 * 2 == 1024 bytes,
   ```

   where `ca` is the client comforting amount, `T` is the buffering time and `ci` is the client comforting interval.
6. If the file does not contain a virus, the Carrier-enabled FortiGate unit sends the rest of the file to the client. If the file is infected, the FortiGate closes the data connection but cannot send a message to the client.

Server comforting

Server comforting can be selected for each protocol.

Similar to client comforting, you can use server comforting to prevent server connection timeouts that can occur while waiting for FortiOS Carrier to buffer and scan large `POST` requests from slow clients.

The **Interval** is the time in seconds before client and server comforting starts after the download has begun, and the time between sending subsequent data.

The **Amount** is the number of bytes sent by client or server comforting at each interval.

Handling oversized MMS messages

Select **Block** or **Pass** for files and email messages exceeding configured thresholds for each protocol.

The oversize threshold refers to the final size of the message, including attachments, after encoding by the client. Clients can use a variety of encoding types; some result in larger file sizes than the original attachment. As a result, a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the oversize threshold.

MM1 sample messages

```
Internet Protocol, Src Addr: 10.128.206.202 (10.128.206.202), Dst Addr: 10.129.192.190
    (10.129.192.190)
Transmission Control Protocol, Src Port: 34322 (34322), Dst Port: http (80), Seq: 1, Ack:
    1, Len: 1380
   Source port: 34322 (34322)
   Destination port: http (80)
   Header length: 20 bytes
   Flags: 0x0010 (ACK)
   Window size: 24840
   Checksum: 0x63c1 (correct)
```

HTTP proxy

```
Hypertext Transfer Protocol
   POST / HTTP/1.1\r\n
```

```
      Request Method: POST
      Request URI: /
      Request Version: HTTP/1.1
   Host: 10.129.192.190\r\n
   Accept: */*, application/vnd.wap.sic,application/vnd.wap.mms-message,text/x-
       hdml,image/mng,image/x-mng,video/mng,video/x-mng,image/bmp\r\n
   Accept-Charset: utf-8,*\r\n
   Accept-Language: en\r\n
   Content-Length: 25902\r\n
   Content-Type: application/vnd.wap.mms-message\r\n
   User-Agent: Nokia7650/1.0 SymbianOS/6.1 Series60/0.9 Profile/MIDP-1.0
       Configuration/CLDC-1.0 UP.Link/6.2.1\r\n
   x-up-devcap-charset: utf-8\r\n
   x-up-devcap-max-pdu: 102400\r\n
   x-up-uplink: magh-ip.mi.vas.omnitel.it\r\n
   x-wap-profile: "http://nds.nokia.com/uaprof/N7650r200.xml"\r\n
   x-up-subno: 1046428312-826\r\n
   x-up-calling-line-id: 393475171234\r\n
   x-up-forwarded-for: 10.211.4.12\r\n
   x-forwarded-for: 10.211.4.12\r\n
   Via: 1.1 magh-ip.mi.vas.omnitel.it\r\n
   \r\n
```

Scan engine

```
MMS Message Encapsulation, Type: m-send-req
   X-Mms-Message-Type: m-send-req (0x80)
   X-Mms-Transaction-ID: 1458481935
   X-Mms-MMS-Version: 1.0
   From: <insert address>
   To: 3475171234/TYPE=PLMN
   X-Mms-Message-Class: Personal (0x80)
   X-Mms-Expiry: 21600.000000000 seconds
   X-Mms-Priority: Normal (0x81)
   X-Mms-Delivery-Report: No (0x81)
   X-Mms-Read-Report: No (0x81)
   Content-Type: application/vnd.wap.multipart.related; start=<1822989907>;
       type=application/smil
      Start: <1822989907>
      Type: application/smil
   Data (Post)
      Multipart body
         Part: 1, content-type: text/plain
            Content-Type: text/plain; charset=iso-10646-ucs-2; name=Ciao.txt
               Charset: iso-10646-ucs-2
               Name: Ciao.txt
            Headers
               Content-Location: Ciao.txt
            Line-based text data: text/plain
               \377\376C\000i\000a\000o\000
[Unreassembled Packet: MMSE]
```

Sender notifications and logging

In most cases you will notify the sender that they are causing problems on the network — either by sending malware content, flooding the network, or some other unwanted activity. The notification assumes the sender is

unaware of their activity and will stop or correct it when notified.

However, senders who are notified may use this information to circumvent administration's precautions. For example if flood notification is set to 1000 messages per minute, a notified user may simply reduce their message to 990 messages per minute if this flood is intentional. For this reason, not all problems include sender notifications.

There are two methods of notifying senders:

- MMS notifications
- Replacement messages

And three details to consider for logging and notifying administrators:

- Logging and reporting
- MMS logging options
- SNMP

MMS notifications

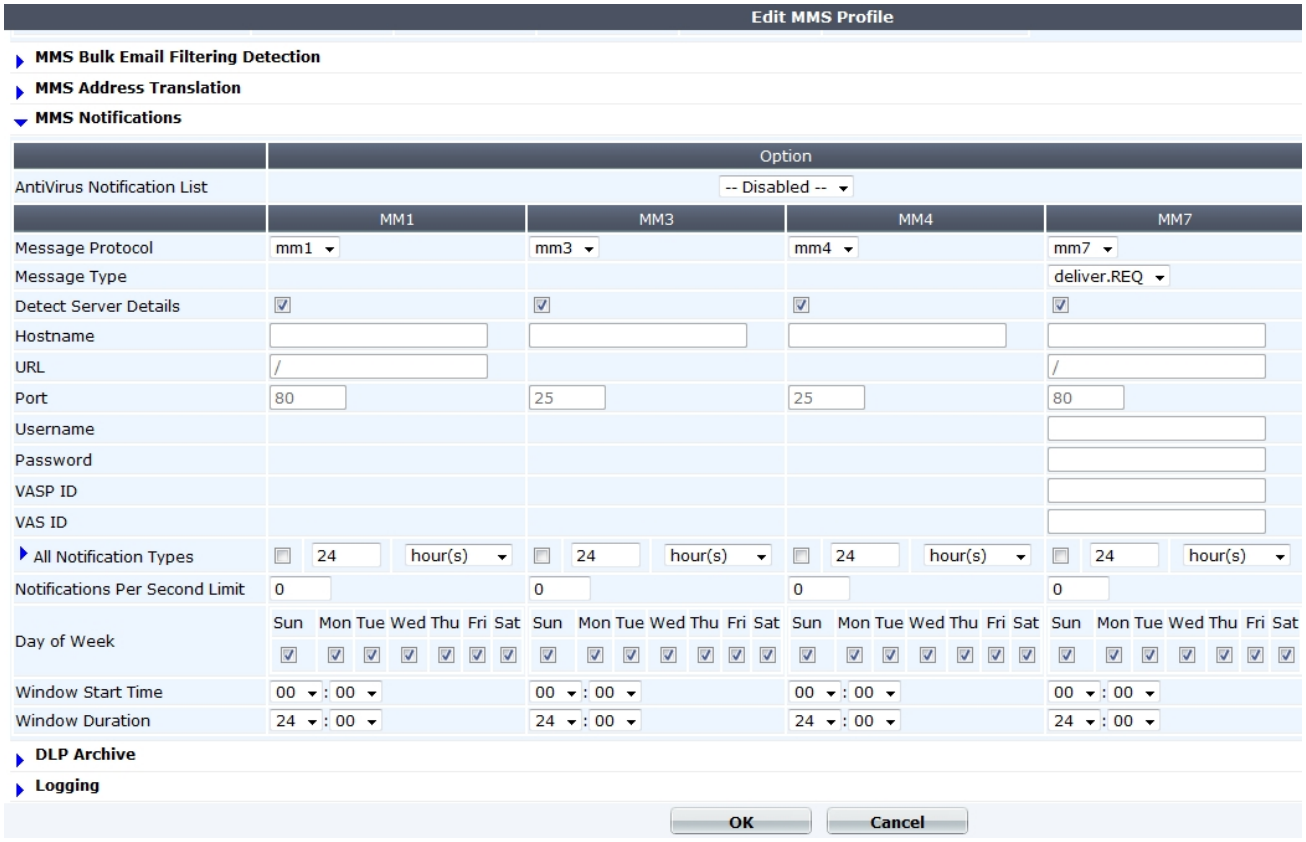
MMS notifications enable you to customize notifications for many different situations and differently for all the supported MMS message protocols — MM1, MM3, MM4, and MM7.

MMS notification types include:

- Content Filter
- File Block
- Carrier Endpoint Block
- Flood
- Duplicate
- MMS Content Checksum
- Virus Scan

Day of Week, **Window start time** and **Window Duration** define what days and what time of day alert notifications will be sent. This allows you to control what alerts are sent on weekends. It also lets you control when to start sending notifications each day. This can be useful if system maintenance is performed at the same time each night — you might want to start alert notifications after maintenance has completed. Another reason to limit the time alert messages are sent could be to limit message traffic to business hours.

Notifications screen for FortiOS Carrier MMS Profile



For MMS Notification options, see MMS Notifications.

Replacement messages

FortiGate units send replacement messages when messages or content is blocked, quarantined, or otherwise diverted from the receiver. In it's place a message is sent to notify the receiver what happened.

With FortiOS Carrier MMS replacement messages, send and receive message types are supported separately and receive their own custom replacement messages. This allows the network to potentially notify both the sender and reciever of the problem.

For example the replacement message **MM1 send-req file block message** is sent to the device that sent one or more files that were banned. The default message that is sent is `This device has sent %%NUM_MSG%% messages containing banned files in the last %%DURATION%% hours.` The two variables are replaced by the appropriate values.

Replacement messages are not as detailed or specific as MMS notifications, but they are also not as complicated to configure. They are also useful when content has been removed from an MMS message that was still delivered.

Logging and reporting

With each virus infection, or file block, a syslog message is generated. The format of this syslog message is similar to:

```
2005-09-22 19:15:47 deviceid=FGT5001ABCDEF1234 logid=0211060ABC type=virus
    subtype=infected level=warning src=10.1.2.3 dst=10.2.3.4 srcintf=port1 dstintf=port2
    service=mm1 status=blocked from="<sending MSISDN>" to="<receiving MSISDN>"
    file="eicar.com.txt" virus="EICAR_TEST_FILE" msg="The file eicar.com.txt is infected
    with EICAR_TEST_FILE. ref
    http://www.fortinet.com/VirusEncyclopedia/search/encyclopediaSearch.do?method=quickSea
    rchDirectly&virusName=EICAR_TEST_FILE"
```

Note that the **from** and **to** fields are samples and not real values.

MMS logging options

You can enable logging in an MMS protection profile to write event log messages when the MMS protection profile options that you have enabled perform an action. For example, if you enable MMS antivirus protection, you could also use the MMS protection profile logging options to write an event log message every time a virus is detected.

To record these log messages you must first configure how the FortiOS Carrier unit stores log messages.

To configure MMS content archiving, go to **Security Profiles > Carrier > MMS Profile**. Select **Create New** or select the **Edit** icon beside an existing profile. Expand **MMS Bulk AntiSpam Detection > Logging**. Complete the fields as described in the following table and select **OK**. For more a detailed list of options, see Logging.

SNMP

A simple SNMP trap will be generated to inform the operators' alerting system that a virus has been detected. This SNMP trap could contain the sending and receiving MSISDN, however the initial solution would reflect the current behavior, i.e. only the fact that a virus has been detected will be communicated.

MMS content-based Antispam protection

Expand **MMS Scanning** and select **Content Filter** in an MMS protection profile to create content filter black/white lists that block or allow MMS messages based on the content of the message.

Overview

A school computer lab may block age-inappropriate content. A place of business may block unproductive content. A public access internet cafe may block offensive and graphic content. Each installation has its own requirements for what content needs to be blocked, and in what language.

FortiOS Carrier provides the ability to create custom local dictionaries, black lists, and white lists in multiple languages enables you to protect your customers from malicious content around the world.

Configurable dictionary

You can create a dictionary of configurable terms and phrases using the CLI. The text of MMS messages will be searched for these terms and phrases. Add content filter lists that contain content that you want to match in MMS messages. For every match found, a score is added. If enough matches are found to set the total score above the configured threshold, the MMS message is blocked.

You can add words, phrases, wild cards and Perl regular expressions to create content patterns that match content in MMS messages. For more on wildcard and regular expressions, see Using wildcards and Perl regular expressions in the UTM guide.

For each pattern you can select **Block** or **Exempt**.

- Block adds an antispam black list pattern. A match with a block pattern blocks a message depending on the score of the pattern and the content filter threshold.
- Exempt adds an antispam white list pattern. A match with an exempt pattern allows the message to proceed through the FortiOS Carrier unit, even if other content patterns in the same content filter list would block it.

If a pattern contains a single word, the FortiOS Carrier unit searches for the word in MMS messages. If the pattern contains a phrase, the FortiOS Carrier unit searches for all of the words in the phrase. If the pattern contains a phrase in quotation marks, the FortiOS Carrier unit searches for the whole phrase.

You can create patterns with Simplified Chinese, Traditional Chinese, Cyrillic, French, Japanese, Korean, Spanish, Thai, or Western character sets.

Black listing

Black listing is the practice of banning entries on the list. For example if an IP address continuously sends viruses, it may be added to the black list. That means any computers that consult that list will not communicate with that IP address.

Sometimes computers or devices can be added to black lists for a temporary problem, such as a virus that is removed when notified. However, as a rule short of contacting the administrator in person to manually be removed form the black list, users have to wait and they generally will be removed after a period without problem.

White listing

White listing is the practice of adding all critical IP addresses to a list, such as company email and web servers. Then if those servers become infected and start sending spam or viruses, those servers are not blocked. This allows the critical traffic through, even if there might be some malicious traffic as well. Blocking all traffic from your company servers would halt company productivity.

Scores and thresholds

Each content pattern incudes a score. When a MMS message is matched with a pattern the score is recorded. If a message matches more than one pattern or matches the same pattern more than once, the score for the message increases. When the total score for a message equals or exceeds the threshold the message is blocked.

The default score for a content filter list entry is 10 and the default threshold is 10. This means that by default a message is blocked by a single match. You can change the scores and threshold so that messages can only be blocked if there are multiple matches. For example, you may only want to block messages that contain the phrase “example” if it appears twice. To do this, add the “example” pattern, set action to block and score to 5. Keep the threshold at 10. If “example” is found twice or more in a message the score adds up 10 (or more) and the message is blocked.

Configuring content-based antispam protection

To apply content-based antispam protection - CLI

```
config webfilter content
   edit <filter_table_number>
      set name <filter_table_name>
      config entries
         edit <phrase or regexp you want to block>
            set action {block | exempt}
            set lang <phrase language>
            set pattern-type {wildcard | regexp}
```

```
        set score <phrase score>
        set status {enable | disable}
    end
end
```

Configuring sender notifications

When someone on the MMS network sends an MMS message that is blocked, in most cases you will notify the sender. Typically an administrator is notified in addition to the sender so action can be taken if required. There are two types of sender notifications available in FortiOS Carrier: MMS notifications, and Replacement Messages.

MMS notifications

MMS notifications to senders are configured in **Security Profiles > Carrier > MMS Profile**, under MMS Notifications.

In this section you can configure up to four different notification recipients for any combination of MM1/3/4/7 protocol MMS messages. Also for MM7 messages the message type can be `submit.REQ` or `deliver.REQ`.

Useful settings include:

- delay in message based on notification type
- limit on notifications per second to prevent a flood
- schedules for notifications
- log in details for MM7 messages.

For more information on MMS notifications, see Notifying message flood senders and receivers and MMS Notifications.

Replacement messages

Replacement messages are features common to both FortiOS and FortiOS Carrier, however FortiOS Carrier has additional messages for the MMS traffic.

While each MMS protocol has its own different rec placement messages, the one common to all MMS protocols is the **MMS blocked content replacement message**. This is the message that the receiver of the message sees when their content is blocked.

MMS DLP archiving

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the FortiOS Carrier configuration. The FortiGuard Analysis and Management server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

You can configure full DLP archiving and summary DLP archiving. Full DLP archiving includes all content, for example, full email DLP archiving includes complete email messages and attachments. Summary DLP archiving includes just the meta data about the content, for example, email message summary records include only the email header.

You can archive MM1, MM3, MM4, and MM7 content.

Configuring MMS DLP archiving

Select DLP archive options to archive MM1, MM3, MM4, and MM7 sessions. For each protocol you can archive just session metadata (**Summary**), or metadata and a copy of the associated file or message (**Full**).

In addition to MMS protection profile DLP archive options you can:

- Archive MM1 and MM7 message floods
- Archive MM1 and MM7 duplicate messages
- Select **DLP archiving** for carrier endpoint patterns in a **Carrier Endpoint List** and select the **Carrier Endpoint Block** option in the **MMS Scanning** section of an MMS Protection Profile

FortiOS Carrier only allows one sixteenth of its memory for transferring content archive files. For example, for Carrier-enabled FortiGate units with 128MB RAM, only 8MB of memory is used when transferring content archive files. Best practices dictate to not enable full content archiving if antivirus scanning is also configured because of these memory constraints.

To configure MMS DLP archiving - web-based manager

1. Go to **Security Profiles > Carrier > MMS Profile**.
2. Select **Create New** or select the **Edit** icon beside an existing profile.
3. Expand **MMS Bulk AntiSpam Detection > Content Archive**.
4. Complete the fields as described in DLP Archive options.
5. Select **OK**.

Viewing DLP archives

You can view DLP archives from the Carrier-enabled FortiGate unit web-based manager. Archives are historical logs that are stored on a log device that supports archiving, such as a FortiAnalyzer unit.

These logs are accessed from either **Log & Report > DLP Archive** or if you subscribed to the FortiCloud service, you can view log archives from there.

The **DLP Archive** menu is only visible if one of the following is true.

- You have configured the FortiGate unit for remote logging and archiving to a FortiAnalyzer unit.
- You have subscribed to FortiCloud.

The following tabs are available when you are viewing DLP archives for one of these protocols.

- **E-mail** to view POP3, IMAP, SMTP, POP3S, IMAPS, SMTPS, and spam email archives.
- **Web** to view HTTP and HTTPS archives.
- **FTP** to view FTP archives.
- **IM** to view AIM, ICQ, MSN, and Yahoo! archives.
- **MMS** to view MMS archives.
- **VoIP** to view session control (SIP, SIMPLE and SCCP) archives.

If you need to view log archives in Raw format, select **Raw** beside the **Column Settings** icon.

Message flood protection

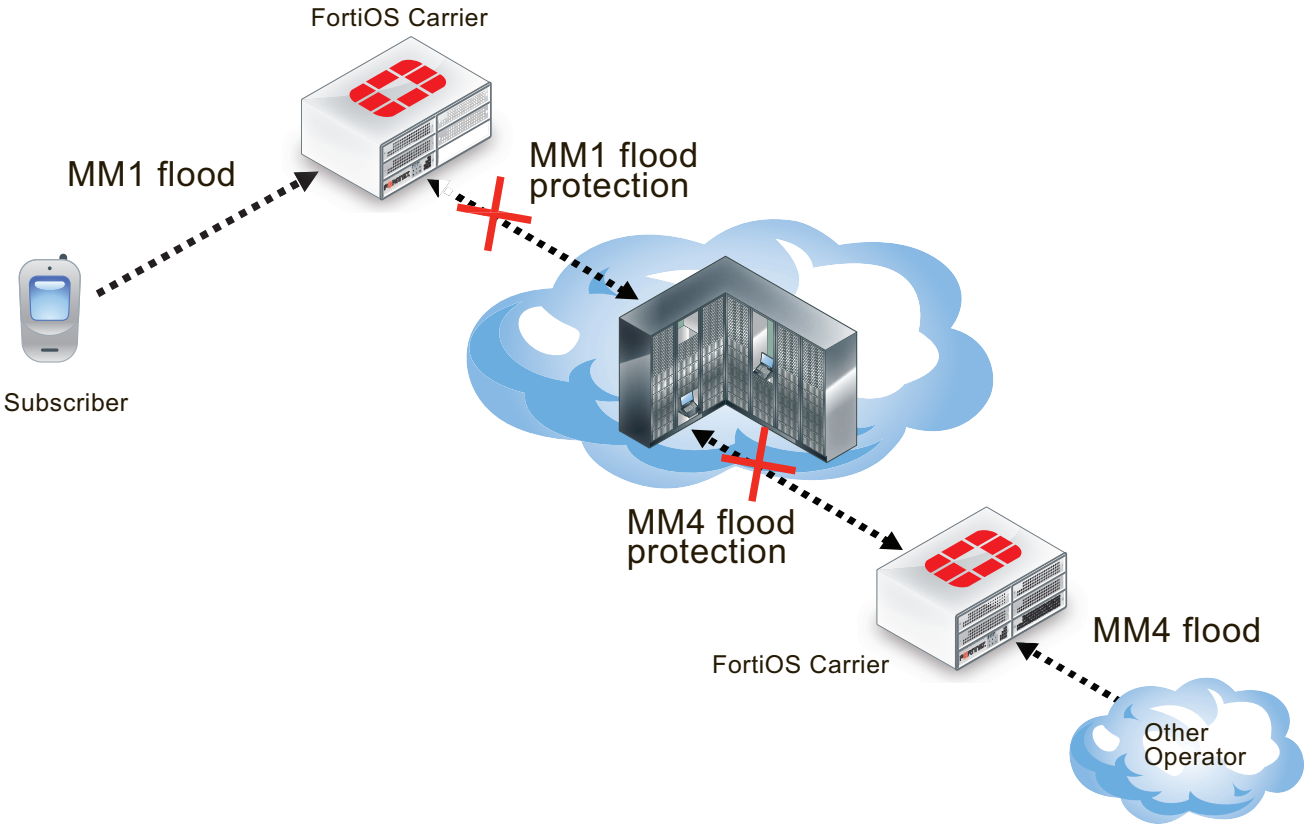
The convenience offered by MM1 and MM4 messaging can be abused by users sending spam or attempting to overload the network with an excess of messages. MMS flood prevention can help prevent this type of abuse.

Overview
Setting message flood thresholds
Notifying administrators of floods
Example — three flood threshold levels with different actions for each threshold
Notifying message flood senders and receivers
Viewing DLP archived messages
Order of operations: flood checking before duplicate checking
Bypassing message flood protection based on user's carrier endpoints
Configuring message flood detection
Sending administrator alert notifications

Overview

Flood protection for MM1 messages prevents your subscribers from sending too many messages to your MMSC. Configuring flood protection for MM4 messages prevents another service provider from sending too many messages from the same subscriber to your MMSC.

MM1 and MM4 flood protection



The FortiOS Carrier unit keeps track of the number of messages each subscriber sends for the length of time you specify. If the number of messages a subscriber sends exceeds the threshold, a configured action is taken. Possible actions are logging the flood, blocking or intercepting messages in the flood, archiving the flood messages, and sending an alert message to inform the administrator that the flood is occurring.

You can create three different thresholds to take different levels of action at different levels of activity.

With this highly configurable system, you can prevent subscribers from sending more messages than you determine is acceptable, or monitor anyone who exceeds the thresholds.

Setting message flood thresholds

A message flood occurs when a single subscriber sends a volume of messages that exceeds the flood threshold you set. The threshold defines the maximum number of messages allowed, the period during which the subscriber sent messages are considered, and the length of time the sender is restricted from sending messages after a flood is detected.

If a subscriber exceeds the message flood threshold and is blocked from sending more messages, any further attempts to send messages will re-start the block period. You must also enable logging for **MMS Scanning > Bulk Messages** in the Logging section of the MMS protection profile.

A subscriber is still able to receive messages while they are blocked from sending messages.

Example

For example, for the first threshold you may determine that any subscriber who sends more than 100 MM1 messages in an hour (60 minutes) will have all messages blocked for half an hour (30 minutes).

Using this example, if the subscriber exceeds the flood threshold, they are blocked from sending message for 30 minutes. If the subscriber tries to send any message after 15 minutes, the message will be blocked and the block period will be reset again to 30 minutes. The block period must expire with no attempts to send a message. Only then will the subscriber be allowed to send more messages.

To configure MM1 message flood threshold - web-based manager

1. Go to **Security Profiles > Carrier > MMS Profile**.
2. Select **Create New**.
3. Enter `MM1 flood` for **Profile Name**.
4. Expand **MMS Bulk Email Filtering Detection**.
5. Enter the following information, and select **OK**.

MM1 (first column)	
Enable	Enable
Message Flood Window	60 minutes
Message Flood Limit	100
Message Flood Block Time	30 minutes
Message Flood Action	Block

To configure MM1 message flood threshold - CLI

```
config firewall mms-profile
   edit profile_name
      config flood mm1
         set status1 enable
         set window1 60
         set limit1 100
         set action1 block
         set block-time1 30
      end
   end
```

The threshold values that you set for your network will depend on factors such as how busy your network is and the kinds of problems that your network and your subscribers encounter. For example, if your network is not too busy you may want to set message flood thresholds relatively high so that only an exceptional situation will exceed a flood threshold. Then you can use log messages and archived MMS messages to determine what caused the flood.

If your subscribers are experiencing problems with viruses that send excessive amounts of messages, you may want to set thresholds lower and enable blocking to catch problems as quickly as possible and block access to keep the problem from spreading.

Flood actions

When the Carrier-enabled FortiGate unit detects a message flood, it can take any combination of the five actions that you can configure for the flood threshold. For detailed options, see Message Flood.

Notifying administrators of floods

You can configure alert notifications for message floods by selecting the Alert Notification message flood action.

The FortiOS Carrier unit sends alert notifications to administrators using the MM1, MM3, MM4, or MM7 content interface. To send an alert notification you must configure addresses and other settings required for the content interface.

For example, to send notifications using the MM1 content interface you must configure a source MSISDN, hostname, URL, and port to which to send the notification. You can also configure schedules for when to send the notifications.

Finally you can add multiple MSISDN numbers to the MMS protection profile and set which flood thresholds to send to each MSISDN.

Example — three flood threshold levels with different actions for each threshold

You can set up to three threshold levels to take different actions at different levels of activity.

The first example threshold records log messages when a subscriber's handset displays erratic behavior by sending multiple messages using MM1 at a relatively low threshold. The erratic behavior could indicate a problem with the subscriber's handset. For example, you may have determined for your network that if a subscriber sends more the 45 messages in 30 minutes that you want to record log messages as a possible indication or erratic behavior.

From the web-based manager in an MMS profile set message **Flood Threshold 1** to:

Enable	Selected
Message Flood Window	30 minutes
Message Flood Limit	45
Message Flood Action	Log

From the CLI:

```
config firewall mms-profile
   edit profile_name
      config flood mm1
         set status1 enable
         set window1 30
         set limit1 45
         set action1 log
      end
```

```
    end
```

Set a second higher threshold to take additional actions when a subscriber sends more that 100 messages in 30 minutes. Set the actions for this threshold to log the flood, archive the message that triggered the second threshold, and block the sender for 15 minutes.

From the web-based manager in an MMS profile set message **Flood Threshold 2** to:

Enable	Selected
Message Flood Window	30 minutes
Message Flood Limit	100
Message Block Time	15 minutes
Message Flood Action	Log, DLP archive First message only, Block

From the CLI:

```
config firewall mms-profile
   edit profile_name
      config flood mm1
         set status2 enable
         set window2 30
         set limit2 100
         set action2 block log archive-first
         set block-time2 15
      end
   end
```

Set the third and highest threshold to block the subscriber for an extended period and sand an administrator alert if the subscriber sends more than 200 messages in 30 minutes. Set the actions for this threshold to block the sender for four hours (240 minutes), log the flood, archive the message that triggered the third threshold, and send an alert to the administrator.

From the web-based manager in an MMS profile set message **Flood Threshold 3** to:

Enable	Selected
Message Flood Window	30 minutes
Message Flood Limit	200
Message Block Time	240 minutes
Message Flood Action	Log, Block, Alert Notification

Because you have selected the **Alert Notification** action you must also configure alert notification settings. For this example, the source MSISDN is 5551234—telephone number 555-1234. When administrators receive MMS messages from this MSIDSN they can assume a message flood has been detected.

In this example, alert notifications are sent by the FortiOS Carrier unit to the MMSC using MM1. The host name of the MMSC is `mmscexample`, the MMSC URL is `/`, and the port used by the MMSC is 80. In this example, the alert notification window starts at 8:00am and extends for eight hours on weekdays (Monday-Friday) and the minimum interval between message flood notifications is two hours.

Source MSISDN	5551234
Message Protocol	MM1
Hostname	mmscexample
URL	/
Port	80
Notifications Per Second Limit	0
Window Start Time	8:00
Window Duration	8:00
Day of Week	Mon, Tue, Wed, Thu, Fri, Sat
Interval	2 hours

From the CLI:

```
config firewall mms-profile
   edit profile_name
      config notification alert-flood-1
         set alert-src-msisdn 5551234
         set set msg-protocol mm1
         set mmsc-hostname mmscexample
         set mmsc-url /
         set mmsc-port 80
         set rate-limit 0
         set tod-window-start 8:00
         set tod-window-duration 8:00
         set days-allowed monday tuesday wednesday thursday friday
         set alert-int 2
         set alert-int-mode hours
   end
```

You must also add the MSISDNs of the administrators to be notified of the message flood. In this example, the administrator flood threshold 3 alert notifications are sent to one administrator with MSISDN 5554321.

To add administrator's MSISDNs for flood threshold 3 from the web-based manager when configuring a protection profile, select **MMS Bulk Email Filtering Detection > Recipient MSISDN > Create New**.

MSISDN	5554321
Flood Level 3	Select

From the CLI:

```
config firewall mms-profile
   edit profile_name
      config notif-msisdn
         edit 5554321
            set threshold flood-thresh-3
      end
end
```

Notifying message flood senders and receivers

The FortiOS Carrier unit does not send notifications to the sender or receiver that cause a message flood. If the sender or receiver is an attacker and is explicitly informed that they have exceeded a message threshold, the attacker may try to determine the exact threshold value by trial and error and then find a way around flood protection. For this reason, no notification is set to the sender or receiver.

However, FortiOS Carrier does have replacement messages for sending reply confirmations to MM1 senders and receivers and for MM4 senders for blocked messages identified as message floods. For information about how FortiOS Carrier responds when message flood detection blocks a message, see and MMS duplicate messages and message floods.

Responses to MM1 senders and receivers

When the FortiOS Carrier unit identifies an MM1 message sent by a sender to an MMSC as a flood message and blocks it, the FortiOS Carrier unit returns a message submission confirmation (`m-send.conf`) to the sender — otherwise the sender's handset would keep retrying the message. The `m-send.conf` message is sent only when the MM1 message flood action is set to Block. For other message flood actions the message is actually delivered to the MMSC and the MMSC sends the `m-send.conf` message.

You can customize the `m-send.conf` message by editing the **MM1 send-conf flood message** MM1 replacement message (from the CLI the `mm1-send-conf-flood` replacement message). You can customize the response status and message text for this message. The default response status is "Content not accepted". To hide the fact that FortiOS Carrier is responding to a flood, you can change the response status to "Success". The default message text informs the sender that the message was blocked. You could change this to something more generic.

For example, the following command sets the submission confirmation response status to "Success" and changes the message text to "Message Sent OK":

```
config system replacemsg mm1 mm1-send-conf-flood
   set rsp-status ok
   set rsp-text "Message Sent OK"
end
```

When the FortiOS Carrier unit identifies an MM1 message received by a receiver from an MMSC as a flood message and blocks it, the FortiOS Carrier unit returns a message retrieval confirmation (m-retrieve.conf) to the sender (otherwise the sender's handset would keep retrying the message). The m-retrieve.conf message is sent only when the MM1 message flood action is set to Block. For other message flood actions the message is actually delivered to the receiver, so the MMSC sends the m-retrieve.conf message.

You can customize the m-retrive.conf message by editing the **MM1 retrieve-conf flood message** MM1 replacement message (from the CLI the `mm1-retr-conf-flood` replacement message). You can customize the class, subject, and message text for this message.

For example, you could use the following command make the response more generic:

```
config system replacemsg mm1 mm1-retr-conf-flood
   set subject "Message blocked"
   set message "Message temporarily blocked by carrier"
end
```

Forward responses for MM4 message floods

When the FortiOS Carrier unit identifies an MM4 message as a flood message and blocks it, the FortiOS Carrier unit returns a message forward response (MM4_forward.res) to the forwarding MMSC (otherwise the forwarding MMSC would keep retrying the message). The MM4_forward.res message is sent only when the MM4 message flood action is set to Block and the MM4-forward.req message requested a response. For more information, see and MMS duplicate messages and message floods.

You can customize the MM4_forward.res message by editing the **MM4 flood message** MM4 replacement message (from the CLI the `mm4-flood` replacement message). You can customize the response status and message text for this message. The default response status is "Content not accepted" (`err-content-not-accept`). To hide the fact that the FortiOS Carrier unit is responding to a flood, you can change the response status to "Success". The default message text informs the sender that the message was blocked. You could change this to something more generic.

For example, the following command sets the submission confirmation response status to "Success" and changes the message text to "Message Sent OK" for the MM4 message forward response

```
config system replacemsg mm4 mm4-flood
   set rsp-status ok
   set rsp-text "Message Forwarded OK"
end
```

Viewing DLP archived messages

If **DLP Archive** is a selected message flood action, the messages that exceed the threshold are saved to the MMS DLP archive. The default behavior is to save all of the offending messages, but you can configure the DLP archive setting to save only the first message that exceeds the threshold. This still provides a sample of the offending messages without requiring as requiring as much storage.

To select only the first message in a flood for DLP archiving - web-based manager

1. Go to **Security Profiles > Carrier > MMS Profile**.
2. Edit an existing MMS Profile.
3. Expand the **MMS Bulk Email Filtering Detection** section, the **Message Flood** subsection, and the desired **Flood Threshold** subsection.
4. Next to **DLP Archive**, select **First message only** from the dropdown menu.
5. Select **OK**.

Order of operations: flood checking before duplicate checking

Although duplicate checking involves only examination and comparison of message contents and not the sender or recipient, and flood checking involves only totalling the number of messages sent by each subscriber regardless of the message content, there are times when a selection of messages exceed both flood and duplicate thresholds.

The Carrier-enabled FortiGate unit checks for message floods before checking for duplicate messages. Flood checking is less resource-intensive and if the flood threshold invokes a **Block** action, the blocked messages are stopped before duplicate checking occurs. This saves both time and FortiOS Carrier system resources.

The duplicate scanner will only scan content. It will not scan headers. Content must be exactly the same. If there is any difference at all in the content, it will not be considered a duplicate.

Bypassing message flood protection based on user's carrier endpoints

You can use carrier endpoint filtering to exempt MMS sessions from message flood protection. Carrier endpoint filtering matches carrier endpoints in MMS sessions with carrier endpoint patterns.

If you add a carrier endpoint pattern to a filter list and set the action to exempt from mass MMS, all messages from matching carrier endpoints bypass message flood protection. This allows legitimate bulk messages, such as system outage notifications, to be delivered without triggering message flood protection.

For more information on carrier endpoints, see the User Authentication chapter of the FortiOS Handbook.

Configuring message flood detection

To have the Carrier-enabled FortiGate unit check for message floods, you must first configure the flood threshold in an MMS profile, select the MMS profile in a security policy. All the traffic examined by the security policy will be checked for message floods according to the threshold values you set in the MMS profile.

Configure the MMS profile - web-based manager

1. Go to **Firewall Objects > MMS Profile**.
2. If you are editing an MMS profile, select the **Edit** icon of the MMS profile.
   If you are creating a new MMS profile, select **Create New** and enter a profile name.
3. Expand **MMS Bulk Email Filtering Detection**.
4. Expand **Message Flood**.
5. Expand **Flood Threshold 1**.
6. Select the **Enable** check box for MM1 messages, MM4 messages, or both.
7. In the **Message Flood Window** field, enter the length of time the Carrier-enabled FortiGate unit will keep track of the number of messages each subscriber sends.
   If the Carrier-enabled FortiGate unit detects the quantity of messages specified in the **Message Flood Limit** sent during the number of minutes specified in the **Message Flood Window**, a message flood is in progress.
8. In the **Message Flood Limit** field, enter the number of messages required to trigger the flood.
9. In the **Message Flood Block Time** field, enter the length of time a user will be blocked from sending messages after causing the message flood.
10. Select the message flood actions the Carrier-enabled FortiGate unit will take when the message flood is detected.
11. Select **OK**.

Configure the security policy - web-based manager

1. Go to **Policy**.
2. Select the **Edit** icon of the security policy that controls the traffic in which you want to detect message floods.
3. Select the **MMS Profile** check box to enable the use of a protection profile.
4. Select the MMS protection profile from the list.
5. Select **OK**.

Sending administrator alert notifications

When message floods are detected, the Carrier-enabled FortiGate unit can be configured to notify you immediately with an MMS message. Enable this feature by selecting Alert Notification in the message flood action. Each message flood threshold can be configured separately.

Configuring how and when to send alert notifications

You can configure different alert notifications for MM1 and MM4 message floods. You can configure the FortiOS Carrier unit to send these alert notifications using the MM1, MM3, MM4, or MM7 content interface. Each of these content interfaces requires alert notification settings that the FortiOS Carrier unit uses to communicate with a server using the selected content interface.

For the MM1 content interface you require:

- The hostname of the server
- The URL of the server (usually “/”)
- The server port (usually 80)

For the MM3 and MM4 content interfaces you require:

- The hostname of the server
- The server port (usually 80)
- The server user domain

For the MM7 content interface you require:

- The message type
- ***submit.REQ*** to send a notification message to the sender in the form of a submit request. The message goes from a VAS application to the MMSC.
- ***deliver.REQ*** to send a notification message to the sender in the form of a deliver request. The message goes from the MMSC to a VAS application.
- The hostname of the server
- The URL of the server (usually “/”)
- The server port (usually 80)
- A user name and password to connect to the server
- The value-added-service-provider (VASP) ID
- The value-added-service (VAS) ID

For more information, see MMS notifications.

To configure administrator alert notifications - web-based manager

1. Go to **Firewall Objects > MMS Profile** and edit or add a new MMS protection profile.
2. Expand **MMS Bulk Email Filtering Detection**.
   There are three message flood thresholds.
3. Expand the threshold that you want to configure alert notification for.
4. For **Message Flood Action**, select the **Alert Notification** check box. Alert notification options appear.
5. For the **Source MSISDN**, enter the MSISDN from which the alert notification message will be sent.
6. Select the Message Protocol the alert notification will use: **MM1**, **MM3**, **MM4**, or **MM7**.
7. Add the information required by FortiOS Carrier to send messages using the selected message protocol:
8. For **Notifications Per Second Limit**, enter the number of notifications to send per second.
   Use this setting to reduce control the number of notifications sent by the FortiOS Carrier unit. If you enter zero (0), the notification rate is not limited.
9. If required, change **Window Start Time** and **Window Duration** configure when the FortiOS Carrier unit sends alert notifications.
   By default, notifications are sent at any time of the day. You can change the Window Start Time if you want to delay sending alert messages. You can also reduce the Window Duration if you want to stop sending alert notifications earlier.

   For example, you might not want FortiOS Carrier sending notifications except during business hours. In this case the Window Start Time could be 9:00 and the Window Duration could be 8:00 hours.

   You can set different alert notifications for each message threshold. For example, you could limit the message window for lower thresholds and set it to 24 hours for higher thresholds. This way administrators will only receive alert notifications outside of business hours for higher thresholds.
10. For **Day of Week**, select the days of the week to send notifications.
    For example, you may only want to send alert notifications on weekends for higher thresholds.
11. In the **Interval field**, enter the maximum frequency that alert notification messages will be sent, in minutes or hours.
    All alerts occurring during the interval will be included in a single alert notification message to reduce the number of alert messages that are sent.

Configuring who to send alert notifications to

In each MMS protection profile you add a list of recipient MSISDNs. For each of these MSISDNs you select the message flood threshold that triggers sending notifications to this MSISDN.

To configure the alert notification recipients - web-based manager

1. Go to **Firewall Objects > MMS Profile**.
2. Select the **Edit** icon of the MMS profile in which you want to configure the alert notification recipients.
3. Expand **MMS Bulk Email Filtering Detection**.
4. Expand **Recipient MSISDN**.
5. Select **Create New**.
6. In the **New MSISDN** window, enter the MSISDN to use for flood threshold alert notification.
7. Select the duplicate thresholds at which to send alert notifications to the MSISDN.

For the flood threshold to be able to send an alert notification to the MSISDN, the alert notification action must be enabled and configured within the flood threshold.

Duplicate message protection

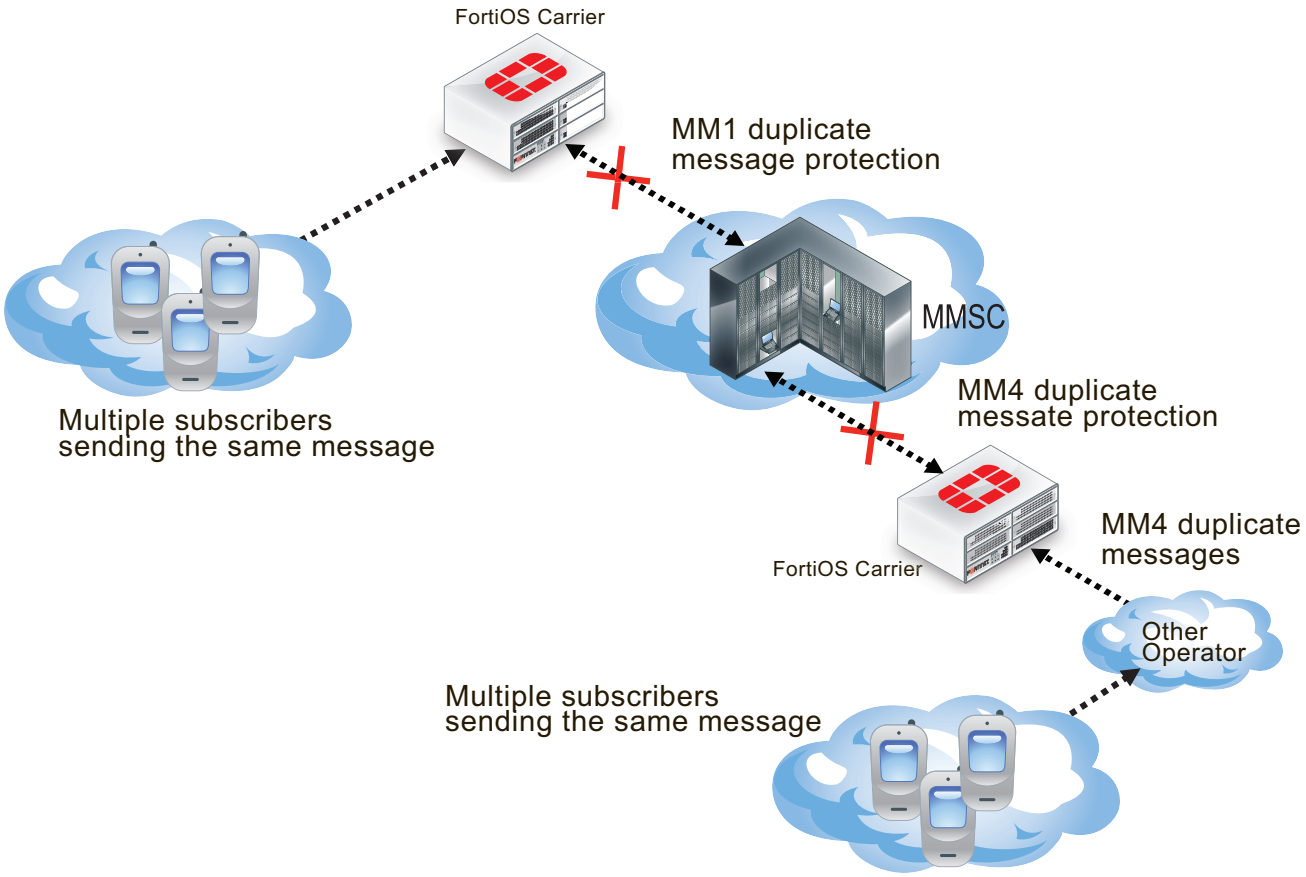
The convenience offered by MM1 and MM4 messaging can be abused by users sending spam or other unwanted messages. Often, the same message will be sent by multiple subscribers. The message can be spam, viral marketing, or worm-generated messages. MMS duplicate prevention can help prevent this type of abuse by keeping track of the messages being sent.

Overview
Using message fingerprints to identify duplicate messages
Messages from any sender to any recipient
Setting duplicate message thresholds
Duplicate message actions
Notifying duplicate message senders and receivers
Viewing DLP archived messages
Order of operations: flood checking before duplicate checking
Bypassing duplicate message detection based on user's carrier endpoints
Configuring duplicate message detection
Sending administrator alert notifications

Overview

Duplicate message protection for MM1 messages prevents multiple subscribers from sending duplicate messages to your MMSC. Duplicate message protection for MM4 messages prevents another service provider from sending duplicate messages from the same subscriber to your MMSC. This can help prevent a potential flood that would otherwise become widespread between carriers.

MM1 and MM4 duplicate message protection



The FortiOS Carrier unit keeps track of the sent messages. If the same message appears more often than the threshold value you configure, then action is taken. Possible actions are logging the duplicates, blocking or intercepting duplicate messages, archiving the duplicate messages, and sending an alert to inform an administrator that duplicates are occurring.

With this highly configurable system, you can prevent the transmission of duplicate messages when there are more than you determine is acceptable.

For detailed configuration options, see Duplicate Message.

Using message fingerprints to identify duplicate messages

The Carrier-enabled FortiGate unit detects duplicates by keeping a record of all the messages travelling on the network and comparing new messages to those that have already been sent.

Rather than save the messages, the FortiOS carrier creates a checksum using the message body and subject. This serves as a fingerprint to identify the message. If another message with the same message body and subject appears, the fingerprint will also be the same and the Carrier-enabled FortiGate unit will recognize it as a duplicate.

By creating and saving message fingerprints instead of saving the messages, the Carrier-enabled FortiGate unit can save resources and time.

Messages from any sender to any recipient

Duplicate message detection will detect duplicate messages regardless of the sender or recipient. To do this, message fingerprints are generated using only the message body and subject. The sender, recipient, and other header information is not included.

If multiple messages appear with the same subject and message body, the Carrier-enabled FortiGate unit will recognize them as being the same.

Setting duplicate message thresholds

The FortiOS Carrier recognizes all duplicate messages, but it will take action when it detects a volume of duplicate messages that exceed the duplicate threshold you set. The threshold defines the maximum number of duplicate messages allowed, the period during which the messages are considered, and the length of time the duplicate message can not be sent by anyone.

For example, you may determine that once a duplicate message is sent more than 300 times in an hour, any attempt to send the same duplicate message will be blocked for 30 minutes.

If a particular duplicate message exceeds the duplicate message threshold and is blocked, any further attempts to send the same message will re-start the block period.

Using the example above, if the duplicate message count exceeds the duplicate threshold, any attempt to send a copy of the duplicate message will be blocked for 30 minutes. If a subscriber tries to send a copy of the message after waiting 15 minutes, the message will be blocked and the block period will be reset to 30 minutes. The block period must expire with no attempts to send a duplicate message. Only then will a subscriber be allowed to send the message. Non-duplicate messages will not reset the block period.

Duplicate message actions

When the Carrier-enabled FortiGate unit detects that a duplicate message has exceeded duplicate threshold, it can take any combination of the five actions you configure for the duplicate threshold.

Action		Description
Log		Add a log entry indicating that a duplicate message event has occurred. You must also enable logging for **MMS Scanning > Bulk Messages** in the **Logging** section of the MMS protection profile.
DLP Archive		
	All messages	Save all the messages that exceed the duplicate threshold in the DLP archive.
	First message only	Save the first message to exceed the duplicate threshold in the DLP archive. Subsequent messages that exceed the duplicate threshold will not be saved.
Intercept		Messages that exceed the duplicate threshold are passed to the recipients, but if quarantine is enabled for intercepted messages, a copy of each message is also quarantined for later examination. If the quarantine of intercepted messages is disabled, the **Intercept** action has no effect.
Block		Messages that exceed the duplicate threshold are blocked and will not be delivered to the message recipients. If quarantine is enabled for blocked messages, a copy of each blocked message is quarantined for later examination.
Alert Notification		If the duplicate threshold is exceeded, the Carrier-enabled FortiGate unit will send an MMS duplicate message notification message.

Notifying duplicate message senders and receivers

The FortiOS Carrier unit does not send notifications to the sender or receiver of duplicate messages. If the sender or receiver is an attacker and is explicitly informed that they have exceeded a message threshold, the attacker may try to determine the exact threshold value by trial and error and then find a way around duplicate message protection. For this reason, no notification is set to the sender or receiver.

However, the FortiOS Carrier unit does have replacement messages for sending reply confirmations to MM1 senders and receivers and for MM4 senders for blocked messages identified as duplicate messages. For information about how FortiOS Carrier responds when message flood detection blocks a message, see and MMS duplicate messages and message floods.

Responses to MM1 senders and receivers

When the FortiOS Carrier unit identifies an MM1 message sent by a sender to an MMSC as a duplicate message and blocks it, the FortiOS Carrier unit returns a message submission confirmation (m-send.conf) to the sender (otherwise the sender's handset would keep retrying the message). The m-send.conf message is sent only when the MM1 duplicate message action is set to Block. For other duplicate message actions the message is actually delivered to the MMSC and the MMSC sends the m-send.conf message.

You can customize the m-send.conf message by editing the **MM1 send-conf duplicate message** MM1 replacement message (from the CLI the `mm1-send-conf-dupe` replacement message). You can customize

the response status and message text for this message. The default response status is “Content not accepted”. To hide the fact that the FortiOS Carrier unit is responding to a duplicate message, you can change the response status to “Success”. The default message text informs the sender that the message was blocked. You could change this to something more generic.

For example, the following command sets the submission confirmation response status to “Success” and changes the message text to “Message Sent OK”:

```
config system replacemsg mm1 mm1-send-conf-dupe
   set rsp-status ok
   set rsp-text "Message Sent OK"
end
```

When the FortiOS Carrier unit identifies an MM1 message received by a receiver from an MMSC as a duplicate message and blocks it, the FortiOS Carrier unit returns a message retrieval confirmation (m-retrieve.conf) to the sender (otherwise the sender’s handset would keep retrying). The m-retrieve.conf message is sent only when the `MM1duplicate` message action is set to Block. For other message flood actions the message is actually received by the receiver, so the MMSC sends the m-retrieve.conf message.

You can customize the m-retrive.conf message by editing the **MM1 retrieve-conf duplicate message** MM1 replacement message (from the CLI the `mm1-retr-conf-dupe` replacement message). You can customize the class, subject, and message text for this message.

For example, you could use the following command make the response more generic:

```
config system replacemsg mm1 mm1-retr-conf-dupe
   set subject "Message blocked"
   set message "Message temporarily blocked by carrier"
end
```

Forward responses for duplicate MM4 messages

When the FortiOS Carrier unit identifies an MM4 message as a duplicate message and blocks it, the FortiOS Carrier unit returns a message forward response (MM4_forward.res) to the forwarding MMSC (otherwise the forwarding MMSC would keep retrying the message). The MM4_forward.res message is sent only when the MM4 duplicate message action is set to Block and the MM4-forward.req message requested a response. For more information, see and MMS duplicate messages and message floods.

You can customize the MM4_forward.res message by editing the **MM4 duplicate message** MM4 replacement message (from the CLI the `mm4-dupe` replacement message). You can customize the response status and message text for this message. The default response status is “Content not accepted” (`err-content-not-accept`). To hide the fact that the FortiOS Carrier unit is responding to a duplicate message, you can change the response status to “Success”. The default message text informs the sender that the message was blocked. You could change this to something more generic.

For example, the following command sets the submission confirmation response status to “Success” and changes the message text to “Message Forwarded OK”:

```
config system replacemsg mm4 mm4-dupe
   set rsp-status ok
   set rsp-text "Message Forwarded OK"
end
```

Viewing DLP archived messages

If **DLP Archive** is a selected duplicate message action, the messages that exceed the threshold are saved to the MMS DLP archive. The default behavior is to save all of the offending messages but you can configure the DLP archive setting to save only the first message that exceeds the threshold. See Viewing DLP archived messages.

Order of operations: flood checking before duplicate checking

Although duplicate checking involves only examination and comparison of message contents and not the sender or recipient, and flood checking involves only totalling the number of messages sent by each subscriber regardless of the message content, there are times when a selection of messages exceed both flood and duplicate thresholds.

The Carrier-enabled FortiGate unit checks for message floods before checking for duplicate messages. Flood checking is less resource-intensive and if the flood threshold invokes a **Block** action, the blocked messages are stopped before duplicate checking occurs. This saves both time and FortiOS Carrier system resources.

Bypassing duplicate message detection based on user's carrier endpoints

You can use carrier endpoint filtering to exempt MMS sessions from duplicate message detection. Carrier endpoint filtering matches carrier endpoints in MMS sessions with carrier endpoint patterns. If you add a carrier endpoint pattern to a filter list and set the action to exempt from mass MMS, all messages from matching carrier endpoints bypass duplicate message detection. For more information about endpoints, see FortiOS Handbook User Authentication guide.

Configuring duplicate message detection

To have the Carrier-enabled FortiGate unit check for duplicate messages, configure the duplicate threshold in an MMS profile, and select the MMS profile in a security policy.

All traffic matching the security policy will be checked for duplicate messages according to the settings in the MMS profile.

The duplicate scanner will only scan content. It will not scan headers. Content must be exactly the same. If there is any difference at all in the content, it will not be considered a duplicate.

The modular nature of the profiles allows you great flexibility in how you configure the scanning options. MMS profiles can be used in any number of policies, with different GTP profiles.

In a complex configuration, there may be many security policies, each with a different MMS profile. For a simpler network, you may have many security policies all using the same MMS profile.

Sending administrator alert notifications

When duplicate messages are detected, the Carrier-enabled FortiGate unit can be configured to notify you immediately with an MMS message. Enable this feature by selecting Alert Notification in the duplicate message action. Each duplicate message threshold can be configured separately.

Configuring how and when to send alert notifications

You can configure different alert notifications for MM1 and MM4 duplicate messages. You can configure the FortiOS Carrier unit to send these alert notifications using the MM1, MM3, MM4, or MM7 content interface. Each of these content interfaces requires alert notification settings that the FortiOS Carrier unit uses to communicate with a server using the selected content interface.

For the MM1 content interface you require:

- The hostname of the server
- The URL of the server (usually "/")
- The server port (usually 80)

For the MM3 and MM4 content interfaces you require:

- The hostname of the server
- The server port (usually 80)
- The server user domain

For the MM7 content interface you require:

- The message type
- **submit.REQ** to send a notification message to the sender in the form of a submit request. The message goes from a VAS application to the MMSC.
- **deliver.REQ** to send a notification message to the sender in the form of a deliver request. The message goes from the MMSC to a VAS application.
- The hostname of the server
- The URL of the server (usually "/")
- The server port (usually 80)
- A user name and password to connect to the server
- The value-added-service-provider (VASP) ID
- The value-added-service (VAS) ID

To configure administrator alert notifications - web-based manager

1. Go to **Security Profiles > Carrier > MMS Profile** and edit or add a new MMS protection profile.
2. Expand **MMS Bulk Email Filtering Detection**.
   There are three duplicate message thresholds.
3. Expand the threshold that you want to configure alert notification for.
4. For **Duplicate Message Action**, select the **Alert Notification** check box. Alert notification options appear.
5. For the **Source MSISDN**, enter the MSISDN from which the alert notification message will be sent.
6. Select the Message Protocol the alert notification will use: **MM1**, **MM3**, **MM4**, or **MM7**.
7. Add the information required by FortiOS Carrier to send messages using the selected message protocol:
8. For **Notifications Per Second Limit**, enter the number of notifications to send per second.
   Use this setting to reduce control the number of notifications sent by the FortiOS Carrier unit. If you enter zero (0), the notification rate is not limited.
9. If required, change **Window Start Time** and **Window Duration** configure when the FortiOS Carrier unit sends alert notifications.

By default, notifications are sent at any time of the day. You can change the Window Start Time if you want to delay sending alert messages. You can also reduce the Window Duration if you want to stop sending alert notifications earlier.

For example, you might not want FortiOS Carrier sending notifications except during business hours. In this case the Window Start Time could be 9:00 and the Window Duration could be 8:00 hours.

You can set different alert notifications for each message threshold. For example, you could limit the message window for lower thresholds and set it to 24 hours for higher thresholds. This way administrators will only receive alert notifications outside of business hours for higher thresholds.

10. For **Day of Week**, select the days of the week to send notifications.
    For example, you may only want to send alert notifications on weekends for higher thresholds.
11. In the **Interval field**, enter the maximum frequency that alert notification messages will be sent, in minutes or hours.
    All alerts occurring during the interval will be included in a single alert notification message to reduce the number of alert messages that are sent.

Configuring who to send alert notifications to

In each MMS protection profile you add a list of recipient MSISDNs. For each of these MSISDNs you select the duplicate threshold that triggers sending notifications to this MSISDN.

To configure the alert notification recipients - web-based manager

1. Go to **Security Profiles > Carrier > MMS Profile**.
2. Select the **Edit** icon of the MMS profile in which you want to configure the alert notification recipients.
3. Expand **MMS Bulk Email Filtering Detection**.
4. Expand **Recipient MSISDN**.
5. Select **Create New**.
6. In the **New MSISDN** window, enter the MSISDN to use for duplicate threshold alert notification.

Select the duplicate thresholds at which to send alert notifications to the MSISDN.

For the duplicate threshold to be able to send an alert notification to the MSISDN, the duplicate message threshold alert notification action must be enabled and configured.

Configuring GTP on FortiOS Carrier

Configuring GTP support on FortiOS Carrier involves configuring a number of areas of features. Some features require longer explanations, and have their own chapters. The other features are addressed here.

GTP support on the Carrier-enabled FortiGate unit
Configuring General Settings on the Carrier-enabled FortiGate unit
Configuring Encapsulated Filtering in FortiOS Carrier
Configuring the Protocol Anomaly feature in FortiOS Carrier
Configuring Anti-overbilling in FortiOS Carrier
Logging events on the Carrier-enabled FortiGate unit

GTP support on the Carrier-enabled FortiGate unit

The FortiCarrier unit needs to have access to all traffic entering and exiting the carrier network for scanning, filtering, and logging purposes. This promotes one of two configurations — hub and spoke, or bookend.

A hub and spoke configuration with the Carrier-enabled FortiGate unit at the hub and the other GPRS devices on the spokes is possible for smaller networks where a lower bandwidth allows you to divide one unit into multiple virtual domains to fill multiple roles on the carrier network. It can be difficult with a single FortiOS Carrier as the hub to ensure all possible entry points to the carrier network are properly protected from potential attacks such as relayed network attacks.

A bookend configuration uses two Carrier-enabled FortiGate units to protect the carrier network between them with high bandwidth traffic. One unit handles traffic from mobile stations, SGSNs, and foreign carriers. The other handles GGSN and data network traffic. Together they ensure the network is secure.

The Carrier-enabled FortiGate unit can access all traffic on the network. It can also verify traffic between devices, and verify that the proper GPRS interface is being used. For example there is no reason for a Gn interface to be used to communicate with a mobile station — the mobile station will not know what to do with the data — so that traffic is blocked.

When you are configuring your Carrier-enabled FortiGate unit's GTP profile, you must first configure the APN. It is critical to GTP communications — no traffic will flow without the APN.

The Carrier-enabled FortiGate unit does more than just forward and route GTP packets over the network. It also performs:

- Packet sanity checking
- GTP stateful inspection
- Protocol anomaly detection and prevention
- HA
- Virtual domain support

Packet sanity checking

The FortiOS Carrier firewall checks the following items to determine if a packet confirms to the UDP and GTP standards:

- GTP release version number — must be 0, 1, or 2
- Settings of predefined bits
- Protocol type
- UDP packet length

If the packet in question does not confirm to the standards, the FortiOS Carrier firewall drops the packet, so that the malformed or forged traffic will not be processed.

GTP stateful inspection

Apart from the static inspection (checking the packet header), the FortiOS Carrier firewall performs stateful inspection.

Stateful inspection provides enhanced security by keeping track of communications sessions and packets over a period of time. Both incoming and outgoing packets are examined. Outgoing packets that request specific types of incoming packets are tracked; only those incoming packets constituting a proper response are allowed through the firewall.

The FortiOS Carrier firewall can also index the GTP tunnels to keep track of them.

Using the enhanced Carrier traffic policy, the FortiOS Carrier firewall can block unwanted encapsulated traffic in GTP tunnels, such as infrastructure attacks. Infrastructure attacks involve attempts by an attacker to connect to restricted machines, such as GSN devices, network management systems, or mobile stations. If these attmpts to connect are detected, they are to be flagged immediately by the firewall .

Protocol anomaly detection and prevention

The FortiOS Carrier firewall detects and optionally drops protocol anomalies according to GTP standards and specific tunnel states. Protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of protocol specifications. These packets are not seen on a production network. Protocol anomaly attacks exploit poor programming practices when decoding packets, and are typically used to maliciously impair system performance or elevate privileges.

FortiOS Carrier also detects IP address spoofing inside GTP data channel.

See Configuring the Protocol Anomaly feature in FortiOS Carrier.

HA

FortiOS Carrier active-passive HA provides failover protection for the GTP tunnels. This means that an active-passive cluster can provide FortiOS Carrier firewall services even when one of the cluster units encounters a problem that would result in complete loss of connectivity for a stand-alone FortiOS Carrier firewall. This failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially for mission-critical environments.

FortiOS HA synchs TCP sessions by default, but UDP sessions are not synchronized by default. However synchronizing a session is only part of the solution if the goal is to continue GTP processing on a synchronized session after a HA switch. For that to be successful we also need to synch the GTP tunnel state. So, once the master completes tunnel setup then the GTP tunnel is synchronized to the slave.

GTP traffic will only flow without interruption on a HA switch if bidirectional GTP policies have been configured: an internal (GTP server) to external (all) UDP port GTP policy, and an external (all) to internal (GTP server) UDP port GTP policy. If either policy is missing then traffic may be interrupted until traffic flows in the opposite direction.

For more information on HA in FortiOS, see the High Availability (HA) Guide or the FortiOS Administration Guide.

Virtual domain support

FortiOS Carrier is suited to both large and smaller carriers. A single Carrier-enabled FortiGate unit can serve either one large carrier, or several smaller ones through virtual domains. As with any FortiGate unit, Carrier-enabled units have the ability to split their resources into multiple virtual units. This allows smaller carriers to use just the resources that they need without wasting the extra. For more information on HA in FortiOS, see the Virtual Domains (VDOMs) Guide.

Configuring General Settings on the Carrier-enabled FortiGate unit

To configure the GTP General Settings, go to **Security Profiles > Carrier > GTP Profile**, and edit a GTP profile. Expand **General Settings** to configure settings. See General settings options.

Configuring Encapsulated Filtering in FortiOS Carrier

Encapsulated traffic on the GPRS network can come in a number of forms as it includes traffic that is “wrapped up” in another protocol. This detail is important for firewalls because it requires “unwrapping” to properly scan the data inside. If encapsulated packets are treated as regular packets, that inside layer will never be scanned and may allow malicious data into your network.

On Carrier-enabled FortiGate units, GTP related encapsulated filtering falls under encapsulated IP traffic filtering, and encapsulated non-IP end user address filtering.

Configuring Encapsulated IP Traffic Filtering

Generally there are a very limited number of IP addresses that are allowed to encapsulate GPRS traffic. For example GTP tunnels are a valid type of encapsulation when used properly. This is the GTP tunnel which uses the Gp or Gn interfaces between SGSNs and GGSNs. However, a GTP tunnel within a GTP tunnel is not accessible — FortiOS Carrier will either block or forward the traffic, but is not able to open it for inspection.

The ability to filter GTP sessions is based on information contained in the data stream and provides operators with a powerful mechanism to control data flows within their infrastructure. You can also configure IP filtering rules to filter encapsulated IP traffic from Mobile Stations.

To configure the Encapsulated IP Traffic Filtering, go to **Security Profiles > Carrier > GTP Profile**, and edit a GTP profile. Expand **Encapsulated IP Traffic Filtering** to configure settings. See Encapsulated IP traffic filtering options.

When to use encapsulated IP traffic filtering

The following are the typical cases that need encapsulated IP traffic filtering:

Mobile station IP pools

In a well-designed network, best practices dictate that the mobile station address pool is to be completely separate from the GPRS network infrastructure range of addresses. Encapsulated IP packets originating from a mobile station will not contain source or destination addresses that fall within the address range of GPRS infrastructures. In addition, traffic originating from the users handset will not have destination/source IP addresses that fall within any Network Management System (NMS) or Charging Gateway (CG) networks.

Communication between mobile stations

Mobile stations on the same GPRS network are not able to communicate with other mobile stations. Best practices dictate that packets containing both source and destination addresses within the mobile station's range of addresses are to be dropped.

Direct mobile device or internet attacks

It may be possible for attackers to wrap attack traffic in GTP protocols and submit the resulting GTP traffic directly to a GPRS network element from their mobile stations or a node on the Internet. It is possible that the receiving SGSN or GGSN would then strip off the GTP header and attempt to route the underlying attack. This underlying attack could have any destination address and would probably have a source address spoofed as if it were valid from that PLMN.

You cannot add an IE removal policy when you are creating a new profile.

Relayed network attacks

Depending on the destination the attack could be directly routed, such as to another node of the PLMN, or rewrapped in GTP for transmission to any destination on the Internet outside the PLMN depending on the routing table of the GSN enlisted as the unwitting relay.

The relayed attack could have any source or destination addresses and could be any of numerous IP network attacks, such as an attack to hijack a PDP context, or a direct attack against a management interface of a GSN or other device within the PLMN. Best practices dictate that any IP traffic originating on the Internet or from an MS with a destination address within the PLMN is to be filtered.

Configuring Encapsulated Non-IP End User Address Filtering

Much of the traffic on the GPRS network is in the form of IP traffic. However some parts of the network do not used IP based addressing, so the Carrier-enabled FortiGate unit is unable to perform Encapsulated IP Traffic Filtering.

Depending on the installed environment, it may be beneficial to detect GTP packets that encapsulate non-IP based protocols. You can configure the FortiOS Carrier firewall to permit a list of acceptable protocols, with all other protocols denied.

The encoded protocol is determined in the PDP Type Organization and PDP Type Number fields within the End User Address Information Element. The PDP Type Organization is a 4-bit field that determines if the protocol is part of the ETSI or IETF organizations. Values are zero and one, respectively. The PDP Type field is one byte long. Both GTP specifications only list PPP, with a PDP Type value of one, as a valid ETSI protocol. PDP Types for the IETF values are determined in the "Assigned PPP DLL Protocol Numbers" sections of RFC 1700. The PDP types are compressed, meaning that the most significant byte is skipped, limiting the protocols listed from 0x00 to 0xFF.

To configure the Encapsulated Non-IP End User Address Filtering, go to **Security Profiles > Carrier > GTP Profile**, and edit a GTP profile. Expand **Encapsulated Non-IP End User Address Filtering** to configure settings. See Encapsulated non-IP end user traffic filtering options.

Configuring the Protocol Anomaly feature in FortiOS Carrier

When anomalies do happen, it is possible for the anomaly to interrupt network traffic or consume network resources — if precautions are not taken. Anomalies can be generated by accident or maliciously, but both methods can have the same results — degrading the performance of the carrier network, or worse.

To configure GTP protocol anomalies, go to **Security Profiles > Carrier > GTP Profile**, and edit a GTP profile. Expand the **Protocol Anomaly** option. SeeProtocol Anomaly prevention options.

The following are some examples:

- The GTP header specifies the length of the packet excluding the mandatory GTP header. In GTP version 0 (GSM 09.60), the mandatory GTP header size is 20 bytes, whereas GTP version 1 (GSM 29.060) specifies that the minimum length of the GTP header is 8 bytes. The GTP packet is composed of the header, followed by Information Elements typically presented in a Type-Length-Value format. It is possible for an attacker to create a GTP packet with a GTP header field length that is incompatible with the length of the necessary information elements.
- The same concepts are true for GTP version 2 headers even though there are different fields in them.
- It is similarly possible for an attacker to create a packet with an invalid IE length. Invalid lengths may cause protocol stacks to allocate incorrect amounts of memory, and thereby cause crashes or buffer overflows.

By default the FortiOS Carrier firewall detects these problems, as well as other protocol anomalies, and drops the packets. All protocol anomaly options are set to **Deny** by default. However, you can change the policy to allow them.

Configuring Anti-overbilling in FortiOS Carrier

GPRS overbilling attacks can be prevented with a properly configured Carrier-enabled FortiGate unit.

Overbilling can occur when a subscriber returns his IP address to the IP pool. Before the billing server closes it, the subscriber's session is still open and vulnerable. If an attacker takes control of the subscriber's IP address, he can send or receive data and the subscriber will be billed for the traffic.

Overbilling can also occur when an available IP address is reassigned to a new mobile station (MS). Subsequent traffic by the previous MS may be forwarded to the new MS. The new MS would then be billed for traffic it did not initiate.

Anti-overbilling with FortiOS Carrier

The Carrier-enabled FortiGate unit can be configured to assist with anti-overbilling measures. These measures ensure that the customer is only billed for connection time and data transfer that they actually use.

Anti-overbilling on the Carrier-enabled FortiGate unit involves:

- the administrator configuring the overbilling settings in the GTP profile to notify the Gi firewall when a GTP tunnel is deleted
- the unit clearing the sessions when the Gi firewall receives a notification from the Gn/Gp firewall about a GTP tunnel being deleted This way, the Gi firewall prevents overbilling by blocking traffic initiated by other users.

The three locations to configure anti-overbilling options include:

- **System > Network > Interface > Gi Gatekeeper** — edit an interface, and enable to monitor Gi anti-overbilling traffic on this interface
- **System > Admin > Settings > Gi Gatekeeper Settings** — set the context ID and port that anti-overbilling will take place on.
- **Security Profiles > Carrier > GTP Profile > Anti-Overbilling** — the IP address, port, interface and context ID to use for anti-overbilling measures.

For detailed options, see Anti-Overbilling options.

Logging events on the Carrier-enabled FortiGate unit

Logging on the Carrier-enabled FortiGate unit is just like logging on any other FortiOS unit. The only difference with FortiOS Carrier is that there are a few additional events that you can log beyond the regular ones. These additional events are covered here.

To enable FortiOS Carrier logging, go to **Log&Report > Event Log**, and ensure **GTP service event** is enabled. Once this option is selected, the logging options under **Security Profiles > Carrier > GTP Profile** will be active.

To change FortiOS Carrier specific logging event settings, go to **Security Profiles > Carrier > GTP Profile** and edit a GTP profile. Expand the **Log** section to change the settings. For detailed options, see Log options.

The following information is contained in each log entry:

Timestamp	The time and date when the log entry was recorded
Source IP address	The sender's IP address.
Destination IP address	The reciever's IP address. The sender-receiver pair includes a mobile phone on the GPRS local network, and a device on a network external to the GPRS network, such as the Internet.
Tunnel Identifier (TID) **Tunnel Endpoint Identifier (TEID)**	An identifier for the start and endpoints of a GTP tunnel. This information uniquely defines all tunnels. It is important for billing information based on the length of time the tunnel was active and how much data passed over the tunnel.
Message type	For available message types, see Common message types on carrier networks.
Packet status	What action was performed on the packet. This field matches the logging options while you are configuring GTP logging. See Anti-overbilling with FortiOS Carrier on page 767. The status can be one of forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited
Virtual domain ID or name	A Carrier-enabled FortiGate unit can be divided into multiple virtual units, each being a complete and self-contained virtual FortiCarrier unit. This field indicates which virtual domain (VDOM) was responsible for the log entry. If VDOMs are not enabled on your unit, this field will be `root`.
Reason to be denied if applicable	If the packet that generated this log entry was denied or blocked, this field will include what part of FortiOS denied or blocked that packet. Such as firewall, antivirus, webfilter, or spamfilter.

An example of the above log message format is for a Tunnel deleted log entry. When a tunnel is deleted, the log entry contains the following information:

- Timestamp
- Interface name (if applicable)
- SGSN IP address (source IP)
- GGSN IP address (destination IP)
- Tunnel ID
- Tunnel duration time in seconds
- Number of messages sent to the SGSN
- Number of messages sent to the GGSN

GTP message type filtering

FortiOS Carrier supports message filtering in GTP by the type of message.

This section includes:

Common message types on carrier networks
Configuring message type filtering in FortiOS Carrier

Common message types on carrier networks

Carrier networks include many types of messages — some concern the network itself, others are content moving across the network, and still others deal with handshaking, billing, or other administration based issues.

GTP contains two major parts GTP for the control plane (GTP-C) and GTP for user data tunnelling (GTP-U). Outside of those areas there are only unknown message types.

GTP-C messages

GTP-C contains the networking layer messages. These address routing, versioning, and other similar low level issues.

When a subscriber requests a Packet Data Protocol (PDP) context, the SGSN will send a create PDP context request GTP-C message to the GGSN giving details of the subscriber's request. The GGSN will then respond with a create PDP context response GTP-C message which will either give details of the PDP context actually activated or will indicate a failure and give a reason for that failure. This is a UDP message on port 212.

GTP-C message types include Path Management Messages, Location Management Messages, and Mobility Management Messages.

Path Management Messages

Path management is used by one GSN to detect if another GSN is alive, or if it has restarted after a failure.

The path management procedure checks if a given GSN is alive or has been restarted after a failure. In case of SGSN restart, all MM and PDP contexts are deleted in the SGSN, since the associated data is stored in a volatile memory. In the case of GGSN restart, all PDP contexts are deleted in the GGSN.

Tunnel Management Messages

The tunnel management procedures are used to create, update, and delete GTP tunnels in order to route IP PDUs between an MS and an external PDN via the GSNs.

The PDP context contains the subscriber's session information when the subscriber has an active session. When a mobile wants to use GPRS, it must first attach and then activate a PDP context. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscriber's access point.

Tunnel management procedures are defined to create, update, and delete tunnels within the GPRS backbone network. A GTP tunnel is used to deliver packets between an SGSN and a GGSN. A GTP tunnel is identified in each GSN node by a TEID, an IP address, and a UDP port number.

Location Management Messages

The location-management procedure is performed during the network-requested PDP context activation procedure if the GGSN does not have an SS7 MAP interface (i.e., Gc interface). It is used to transfer location messages between the GGSN and a GTP-MAP protocol-converting GSN in the GPRS backbone network.

Location management subprocedures are used between a GGSN that does not support an SS7 MAP interface (i.e., Gc interface) and a GTP-MAP protocol-conversing GSN. This GSN supports both Gn and Gc interfaces and is able to perform a protocol conversing between GTP and MAP.

Mobility Management Messages

The MM procedures are used by a new SGSN in order to retrieve the IMSI and the authentication information or MM and PDP context information in an old SGSN. They are performed during the GPRS attach and the inter-SGSN routing update procedures.

The MM procedures are used between SGSNs at the GPRS-attach and inter-SGSN routing update procedures. An identity procedure has been defined to retrieve the IMSI and the authentication information in an old SGSN. This procedure may be performed at the GPRS attach. A recovery procedure enables information related to MM and PDP contexts in an old SGSN to be retrieved. This procedure is started by a new SGSN during an inter-SGSN RA update procedure.

GTP-U messages

GTP-U is focused on user related issues including tunneling, and billing. GTP-U message types include MBMS messages, and GTP-U and Charging Management Messages

MBMS messages

Multimedia Broadcast and Multicast Services (MBMS) have recently begun to be offered over GSM and UMTS networks on UTRAN and GERAN radio access technologies. MBMS is mainly used for mobile TV, using up to four GSM timeslots for one MBMS connection. One MBMS packet flow is replicated by GGSN, SGSN and RNCs.

MBMS is split into the MBMS Bearer Service and the MBMS User Service. The MBMS User Service is basically the MBMS Service Layer and offers a Streaming- and a Download Delivery Method. The Streaming Delivery method can be used for continuous transmissions like Mobile TV services. The Download Method is intended for "Download and Play" services.

GTP-U and Charging Management Messages

SGSNs and GGSNs listen for GTP-U messages on UDP port 2152.

GTP‘ (GTP prime) is used for billing messages. It uses the common GTP messages (GTP Version Not Supported, Echo Request and Echo Response) and adds additional messages related to billing procedures.

Unknown Action messages

If the system doesn’t know what type of message it is, it falls into this category. This is an important category of message because malformed messages may appear and need to be handled with security in mind.

Fortinet best practices dictate that you set **Unknown Action messages** to deny for security reasons.

Configuring message type filtering in FortiOS Carrier

GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry General Packet Radio Service (GPRS) traffic within Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. It allows carriers to transport actual cellular packets over their network via tunneling.

In the CLI, there is a keyword for each type of GTP message for both message filtering, and for message rate limiting.

GTP message rate limiting is only accessible from the CLI using the command `configure firewall gtp`.

To configure GTP message type filtering - web-based manager

1. Go to **Security Profiles > Carrier > GTP Profile**.
2. Select **Create New**.
3. Enter a name for this profile such as `msg_type_filtering`.
4. Select **Message Type Filtering** to expand it.
5. For each type of message in the list, select Allow or Deny. All messages are set to Allow by default.

Fortinet best practices dictate that the unknown message action should be set to **Deny** for security reasons as this will block malformed messages.

6. Optionally select and configure any other GTP features for this profile, such as logging.
7. Select **OK** to save the profile.
8. Apply the `msg_type_filtering` profile a security policy configured for GTP tunnel traffic.

To configure GTP message filtering and block Unknown Message Action messages- CLI

```
config firewall gtp
   edit msg_type_filtering
      config message-filter
         set unknown-message-action deny
      next
   end
end
```

Message Type Fields

Each of the following message types can be allowed or denied by your Carrier-enabled FortiGate unit depending on your carrier network and GTP traffic.

Unknown Message Action

Set this message type to deny.

Many attempts to hack into a carrier network will result in this unknown message type and therefore it is denied for security reasons.

Path Management Messages

Message Type	Used by	Description
Echo Request/Response	GTP-C, GTP-U, GTP'	Echo Request is sent on a path to another GSN to determine if the other node is alive. Echo Response is the reply.
Version not Supported	GTP-C, GTP-U, GTP'	There are multiple versions of GTP. Both devices communicating must use the same version of GTP, or this message will be the response.
Support Extension Headers Notification		Extensions are optional parts that a device can choose to support or not. If a device includes these extensions, it must include headers for the extensions to sure ensure proper formatting.

Tunnel Management Messages

Message Type	Used by	Description
Create PDP Context Request/ Response	GTP-C	Sent from an SGSN to a GGSN node as part of a GPRS PDP Context Activation procedure or the Network-Requested PDP Context Activation procedure. A valid request initiates the creation of a tunnel.
Update PDP Context Request/ Response	GTP-C	Used when PDP Context information changes, such as when a mobile device changes location.
Delete PDP Context Request/ Response	GTP-C	Used to terminate a PDP Context, and confirm the context has been deleted.
Create AA PDP Context Request/ Response	GTP-C	Sent as part of the GPRS Anonymous Access PDP Context Activation. It is used to create a tunnel between a context in the SGSN and a context in the GGSN.
Delete AA PDP Context Request/ Response	GTP-C	Sent as part of the GPRS PDP Anonymous Access Context Deactivation procedure to deactivate an activated PDP Context. It contains Cause and Private Extension Information Elements
Error Indication	GTP-U	Sent to the GGSN when a tunnel PDU is received for the following conditions: — No PDP context exists — PDP context is inactive — No MM context exists — GGSN deletes its PDP context when the message is received.
PDU Notification Request/ Response/ Reject Request/ Reject Response	GTP-C	When receiving a Tunneled PDU (T-PDU), the GGSN checks if a PDP context is established for the given PDP address. If no PDP context has been established, the GGSN may initiate the Network-requested PDP Context Activation procedure by sending a PDU Notification Request to the SGSN. **Reject Request -** Sent when the PDP context requested by the GGSN cannot be established.

Location Management Messages

Message Type	Used By	Description
Send Routing Information for GPRS Request/ Response	GTP-C	Sent by the GGSN to obtain location information for the MS. This message type contains the IMSI of the MS and Private Extension.
Failure Report Request/ Response	GTP-C	Sent by the GGSN to the HLR when a PDU reject message is received. The GGSN requests the HLR to set the flag and add the GGSN to the list of nodes to report to when activity from the subscriber that owns the PDP address is detected. The message contains the subscriber IMSI and Private Extension
Note MS GPRS Present Request/ Response	GTP-C	When the HLR receives a message from a mobile with MDFG set, it clears the MDFG and sends the Note MS Present message to all GGSN's in the subscriber's list. This message type contains subscriber IMSI, GSN Address and Private Extension

Mobility Management Messages

Message Type	Used By	Description
Identification Request/Response	GTP-C	Sent by the new SGSN to the old SGSN to request the IMSI for a MS when a GPRS Attach is done with a P-TMSI and the MS has changed SGSNs since the GPRS Detach was done.
SGSN context Request/ Response/ Acknowledge	GTP-C	Sent by the new SGSN to the old SGSN to request the MM and PDP Contexts for the MS.
Forward Relocation Request/ Response/ Complete/ Complete Acknowledge	GTP-C	Indicates mobile activation/deactivation within a Routing Area. This prevents paging of a mobile that is not active (visited VLR rejects calls from the HLR or applies Call Forwarding). Note that the mobile station does not maintain an attach/detach state. SRNS contexts contain for each concerned RAB the sequence numbers of the GTP-PDUs next to be transmitted in uplink and downlink directions.
Relocation Cancel Request/ Response	GTP-C	Send to cancel the relocation of a connection.
Forward SRNS Context/ Context Acknowledge	GTP-C	This procedure may be used to trigger the transfer of SRNS contexts from RNC to CN (PS domain) in case of inter system forward handover.
RAN Information Relay	GTP-C	Forward the Routing Area Network (RAN) information. A Routing Area (RA) is a subset of a GSM Location Area (LA). A RA is served by only one SGSN. Ensures that regular radio contact is maintained by the mobile

MBMS messages

Message Type	Used By	Description
MBMS Notification Request/ Response/ Reject Request/ Reject Response	GTP-C	Notification of the radio access devices.
Create MBMS Context Request/ Response	GTP-C	Request to create an active MBMS context. The context will be pending until the response is received. Once active, the MBMS context allows the MS to receive data from a specific MBMS source
Update MBMS Context Request/ Response	GTP-C	
Delete MBMS Context Request/ Response	GTP-C	Request to deactivate the MBMS context. When the response is received, the MBMS context will be inactive.

GTP-U and Charging Management Messages

Message Type	Used By	Description
G-PDU	GTP-C, GTP-U	GPRS Packet data unit delivery message.
Node Alive Request/Response	GTP-C, GTP-U	Used to inform rest of network when a node starts service.
Redirection Request/Response	GTP-C, GTP-U	Used to divert the flow of CDRs from the CDFs to another CGF when the sender is being removed, or they are used when the CGF has lost its connection to a downstream system.
Data Record Transfer Request/Response	GTP-C, GTP-U	Used to reliably transport CDRs from the point of generation (SGSN/GGSN) to non-volatile storage in the CGF

GTP identity filtering

FortiOS Carrier supports a number of filtering methods based on subscriber identity such as APN filtering, IMSI filtering, and advanced filtering.

This section includes:

IMSI on carrier networks
Other identity and location based information elements
Configuring APN filtering in FortiOS Carrier
Configuring IMSI filtering in FortiOS Carrier
Configuring advanced filtering in FortiOS Carrier

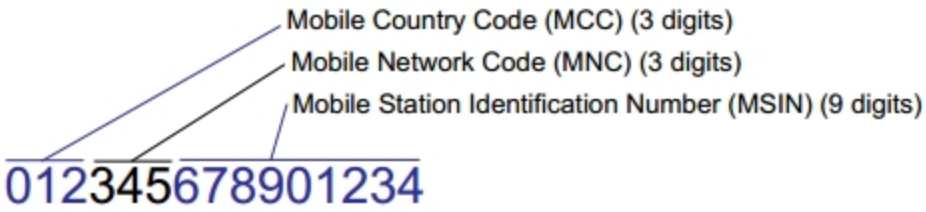
IMSI on carrier networks

The International Mobile Subscriber Identity (IMSI) number is central to identifying users on a carrier network. It is a unique number that is assigned to a cell phone or mobile device to identify it on the GMS or UTMS network.

Typical the IMSI number is stored on the SIM card of the mobile device and is sent to the network as required.

An IMSI number is 15 digits long, and includes the Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Station Identification Number (MSIN).

IMSI codes



The Home Network Identity (HNI) is made up of the MCC and MNC. The HNI is used to fully identify a user's home network. This is important because some large countries have more than one country code for a single carrier. For example a customer with a mobile carrier on the East Coast of the United States would have a different MCC than a customer on the West Coast with the same carrier because even through the MNC would be the same the MCC would be different — the United States uses MCCs 310 to 316 due to its size.

If an IMSI number is not from the local carrier's network, IMSI analysis is performed to resolve the number into a Global Title which is used to access the user's information remotely on their home carrier's network for things like billing and international roaming.

Other identity and location based information elements

IMSI focuses on the user, their location, and carrier network. There are other numbers used to identify different user related Information Elements (IE).

These identity and location based elements include:

- Access Point Number (APN)
- Mobile Subscriber Integrated Services Digital Network (MSISDN)
- Radio Access Technology (RAT) type
- User Location Information (ULI)
- Routing Area Identifier (RAI)
- International Mobile Equipment Identity (IMEI)

Access Point Number (APN)

The Access Point Number (APN) is used in GPRS networks to identify an IP packet data network that a user wants to communicate with. The Network Identifier describes the network and optionally the service on that network that the GGSN is connected to. The APN also includes the MCC and MCN, which together locate the network the GGSN belongs to. An example of an APN in the Barbados using Digicel as the carrier that is connecting to the Internet is `internet.mcc342.mnc750.gprs`.

When you are configuring your Carrier-enabled FortiGate unit's GTP profiles, you must first configure the APN. It is critical to GTP communications and without it no traffic will flow.

The access point can then be used in a DNS query to a private DNS network. This process (called APN resolution) gives the IP address of the GGSN which serves the access point. At this point a PDP context can be activated.

Mobile Subscriber Integrated Services Digital Network (MSISDN)

This is a 15-digit number that, along with the IMSI, uniquely identifies a mobile user. Normally this number includes a 2-digit country code, a 3-digit national destination code, and a 10-digit subscriber number or the phone number of the mobile device, and because of that may change over time if the user changes their phone number. The MSISDN number follows the ITU-T E.164 numbering plan.

Radio Access Technology (RAT) type

The RAT type represents the radio technology used by the mobile device. This can be useful in determining what services or content can be sent to a specific mobile device. FortiOS Carrier supports:

- **UMTS Terrestrial Radio Access Network (UTRAN)**, commonly referred to as 3G, routes many types of traffic including IP traffic. This is one of the faster types.
- **GSM EDGE Radio Access Network (GERAN)** is a key part of the GSM network which routes both phone calls and data.
- **Wireless LAN (WLAN)** is used but not as widely as the other types. It is possible for the mobile device to move from one WLAN to another such as from an internal WLAN to a commercial hot spot.
- **Generic Access Network (GAN)** can also be called unlicensed mobile access (UMA). It routes voice, data, and SIP over IP networks. GAN is commonly used for mobile devices that have a dual-mode and can hand-off between GSM and WLANs.
- **High Speed Packet Access (HSPA)** includes two other protocols High Speed Downlink and Uplink Packet Access protocols (HSDPA and HSUPA respectively). It improves on the older WCDMA protocols by better using the radio bandwidth between the mobile device and the radio tower. This results in an increased data transfer rate for the user.

RAT type is part of advanced filtering configuration. See Configuring advanced filtering in FortiOS Carrier.

User Location Information (ULI)

Gives Cell Global Identity/Service Area Identity (CGI/SAI) of where the mobile station is currently located. The ULI and the RAI are commonly used together to identify the location of the mobile device.

ULI is part of advanced filtering configuration. See Configuring advanced filtering in FortiOS Carrier.

Routing Area Identifier (RAI)

Routing Areas (RAs) divide the carrier network and each has its own identifier (RAI). When a mobile device moves from one routing area to another, the connection is handled by a different part of the network. There are normally multiple cells in a routing area. There is only one SSGN per routing area. The RAI and ULI are commonly used to determine a user's location.

RAI is part of advanced filtering configuration. See Configuring advanced filtering in FortiOS Carrier.

International Mobile Equipment Identity (IMEI)

IMEI is a unique 15-digit number used to identify mobile devices on mobile networks. It is very much like the MAC address of a TCP/IP network card for a computer. It can be used to prevent network access by a stolen phone — the carrier knows the mobile phone's IMEI, and when it is reported stolen that IMEI is blocked from accessing the carrier network no matter if it has the same SIM card as before or not. It is important to note that the IMEI stays with the mobile phone or device where the other information is either location based or stored on the removable SIM card.

IMEI type is part of advanced filtering configuration. See Configuring advanced filtering in FortiOS Carrier.

When to use APN, IMSI, or advanced filtering

At first glance APN, IMSI, and advanced filtering have parts in common. For example two can filter on APN, and another two can filter on IMSI. The difficulty is knowing when to use which type of filtering.

Identity filtering comparison

Filtering type	Filter on the following data:	When to use this type of filtering
APN	APN	Filter based on GTP tunnel start or destination
IMSI	IMSI, MCC-MNC	Filter based on subscriber information
Advanced	PDP context, APN, IMSI, MSISDN, RAT type, ULI, RAI, IMEI	When you want to filter based on: • user phone number (MSISDN) • what wireless technology the user employed • to get on the network (RAT type) • user location (ULI and RAI) • handset ID, such as for stolen phones (IMEI)

APN filtering is very specific — the only identifying information that is used to filter is the APN itself. This will always be present in GTP tunnel traffic, so all GTP traffic can be filtered using this value.

IMSI filtering can use a combination of the APN and MCC-MNC numbers. The MCC and MNC are part of the APN, however filtering on MCC-MNC separately allows you to filter based on country and carrier instead of just the destination of the GTP Tunnel.

Advanced filtering can go into much deeper detail covering PDP contexts, MSISDN, IMEI, and more not to mention APN, and IMSI as well. If you can't find the information in APN or IMSI that you need to filter on, then use Advanced filtering.

Configuring APN filtering in FortiOS Carrier

To configure APN filtering go to **Security Profiles > Carrier > GTP Profile**. Select a profile or create a new one, and expand **APN filtering**.

When you are configuring your Carrier-enabled FortiGate unit's GTP profiles, you must first configure the APN. It is critical to GTP communications and without it no traffic will flow.

Enable APN Filter	Select to enable filtering based on APN value.
Default APN Action	Select either Allow or Deny for all APNs that are not found in the list. The default is Allow.
Value	Displays the APN value for this entry. Partial matches are allowed using wildcard. For example `*.mcc333.mcn111.gprs` would match all APNs from country `333` and carrier `111` on the gprs network.
Mode	Select one or more of the methods used to obtain APN values. Mobile Station provided - The APN comes from the mobile station where the mobile device connected. This is the point of entry into the carrier network for the user's connection. Network provided - The APN comes from the carrier network. Subscription Verified - The user's subscription has been verified for this APN. This is the most secure option.
Action	One of allow or deny to allow or block traffic associated with this APN.
Delete icon	Select to remove this APN entry from the list.
Edit icon	Select to change the information for this APN entry.
Add APN	Select to add an APN to the list. Not active while creating GTP profile, only when editing an existing GTP profile. Save all changes before adding APNs. A warning to this effect will be displayed when you select the **Add APN** button.

The Add APN button is not activated until you save the new GTP profile. When you edit that GTP profile, you will be able to add new APNs.

Configuring IMSI filtering in FortiOS Carrier

In many ways the IMSI on a GPRS network is similar to an IP address on a TCP/IP network. Different parts of the number provide different pieces of information. This concept is used in IMSI filtering on FortiOS Carrier.

To configure IMSI filtering go to **Security Profiles > Carrier > GTP Profile** and expand **IMSI filtering**.

While both the APN and MCC-MCN fields are optional, without using one of these fields the IMSI entry will not be useful as there is no information for the filter to match.

Enable IMSI Filter	Select to turn on IMSI filtering.
Default IMSI Action	Select Allow or Deny. This action will be applied to all IMSI numbers except as indicated in the IMSI list that is displayed. The default value is Allow.
APN	The Access Point Number (APN) to filter on. This field is optional.
MCC-MNC	The Mobile Country Code (MCC) and Mobile Network Code (MNC) to filter on. Together these numbers uniquely identify the carrier and network of the GGSN being used. This field is optional.
Mode	Select the source of the IMSI information as one or more of the following: **Mobile Station provided -** the IMSI number comes from the mobile station the mobile device is connecting to. **Network provided -** the IMSI number comes from the GPRS network which could be a number of sources such as the SGSN, or HLR. **Subscription Verified -** the IMSI number comes from the user's home network which has verified the information. While Subscription Verified is the most secure option, it may not always be available. Selecting all three options will ensure the most complete coverage.
Action	Select the action to take when this IMSI information is encountered. Select one of Allow or Deny.
Delete Icon	Select the delete icon to remove this IMSI entry.
Edit Icon	Select the edit icon to change information for this IMSI entry.
Add IMSI	Select to add an IMSI to the list. Not active while creating GTP profile, only when editing an existing GTP profile. Save all changes before adding IMSIs. A warning to this effect will be displayed when you select the **Add IMSI** button.

Configuring advanced filtering in FortiOS Carrier

Compared to ADN or IMSI filtering, advanced filtering is well named. Advanced filtering can be viewed as a catch-all filtering option — if ADN or IMSI filtering doesn't do what you want, then advanced filtering will. The advanced filtering can use more information elements to provide considerably more granularity for your filtering.

Enable	Select to turn on advanced filtering.
Default Action	Select Allow or Deny as the default action to take when traffic does not match an entry in the advanced filter list .
Messages	Optionally select one or more types of messages this filter applies to: Create PDP Context Request, Create PDP Context Response, Update PDP Context Request, or Update PDP Context Response. Selecting **Create PDP Context Response** or **Update PDP Context Response limits RAT type to only GAN and HSPA, and disables the APN, APN Mode, IMSI, MSISDN, ULI, RAI,** and **IMEI fields.** To select **Update PDP Context Request**, **APN Restriction** must be set to **all**. Selecting **Update PDP Context Request disables the APN, MSISDN,** and **IMEI fields.** if all message types are selected, only the RAT Types of GAN and HSPA are available to select.
APN Restriction	APN Restriction either allows all APNs or restricts the APNs to one of four categories — Public-1, Public-2, Private-1, or Private-2. This can also be combined with a specific APN or partial APN as well as specifying the APN mode.
RAT Type	Select one or more of the Radio Access Technology Types listed. These fields control how a user accesses the carrier's network. You can select one or more of UTRAN, GERAN, WLAN, GAN, HSPA, or any.
ULI	The user location identifier. Often the ULI is used with the RAI to locate a user geographically on the carrier's network. The ULI is disabled when **Create PDP Context Response** or **Update PDP Context Response** messages are selected.
RAI	The router area identifier. There is only one SGSN per routing area on a carrier network. This is often used with ULI to locate a user geographically on a carrier network. The RAI is disabled when **Create PDP Context Response** or **Update PDP Context Response** messages are selected.
IMEI	The International Mobile Equipment Identity. The IMEI uniquely identifies mobile hardware, and can be used to block stolen equipment. The IMEI is only available when **Create PDP Context Request** or no messages are selected.

Action	Select **Allow** or **Deny** as the action when this filter matches traffic. The default is Allow.
Delete Icon	Select to delete this entry from the list.
Edit Icon	Select to edit this entry.
Add	Select to add an advanced filter to the list. Not active while creating GTP profile, only when editing an existing GTP profile. Save all changes before adding advanced filters. A warning to this effect will be displayed when you select the **Add** button.

Troubleshooting

This section offers troubleshooting options for Carrier-related issues.

This section includes:

FortiOS Carrier diagnose commands
Applying IPS signatures to IP packets within GTP-U tunnels
GTP packets are not moving along your network

FortiOS Carrier diagnose commands

This section includes diagnose commands specific to FortiOS Carrier features such as GTP.

GTP related diagnose commands

This CLI command allows you to gain information on GTP packets, logs, statistics, and other information.

```
diag firewall gtp <command>
```

apn list <gtp_profile>	The APN list entries in the specified GTP profile
auth-ggsns show <gtp_profile>	The authorized GGSNs entries for the specified GTP profile. Any GGSNs not on this list will not be recognized.
auth-sgsns show <gtp_profile>	The authorized SGSNs list entries for the specified GTP profile. Any SGSNs not on this list will not be recognized.
handover-grp show <gtp_profile>	The handover group showing the range of allowed handover group IP addresses. The handover group acts like a whitelist of allowed GTP addresses with a default deny at the end — if the GTP address is not on the list, it is denied.
ie-remove-policy list <gtp_profile>	List of IE policies in the IE removal policy for this GTP profile. The information displayed includes the message count for this policy, the length of the SGSN, the list of IEs, and list of SGSN IP addresses.
imsi list <gtp_profile>	IMSI filter entries for this GTP profile. The information displayed includes the message count for this filter, length of the IMSI, the length of the APN and IMSI, and of course the IMSI and APN values.
invalid-sgsns-to-long list <gtp_profile>	List of SGSNs that do not match the filter criteria. These SGSNs will be logged.
ip-policy list <gtp_profile>	List the IP policies including message count for each policy, the action to take, the source and destination IP addresses or ranges, and masks.
noip-policy <gtp_profile>	List the non-IP policies including the message count, which mode, the action to take, and the start and end protocols to be used by decimal number.
path {list | flush}	Select list or flush. List the GTP related paths in FortiOS Carrier memory. Flush the GTP related paths from memory.
policy list <gtp_policy>	The GTP advanced filter policy information for this GTP profile. The information displayed for each entry includes a count for messages matching this filter, a hexidecimal mask of which message types to match, the associated flags, action to take on a match, APN selection mode, MSISDN, RAT types, RAI, ULI, and IMEI.
profile list	Displays information about the configured GTP profiles. You will not be able to see the bulk of the information if you do not log the output to a file.
runtime-stat flush	Select to flush the GTP runtime statistics from memory.

stat	Display the GTP runtime statistics — details on current GTP activity. This information includes how many tunnels are active, how many GTP profiles exist, how many IMSI filter entries, how many APN filter entries, advanced policy filter entries, IE remove policy filter entries, IP policy filter entries, clashes, and dropped packets.
tunnel {list | flush}	Select one of list or flush. List lists all the GTP tunnels currently active. Flush clears the list of active GTP tunnels. This does not clear the clash counter displayed in the `stat` command.

Applying IPS signatures to IP packets within GTP-U tunnels

GTP-U (GTP user data tunnelling) tunnels carry user data packets, signalling messages and error information. GTP-U uses UDP port 2152. Carrier-enabled FortiGate units can apply IPS intrusion protection and detection to GTP-U user data sessions.

To apply IPS to GTP-U user data sessions, add an IPS Sensor to a profile and add the profile to a security policy that accepts GTP-U tunnels. The security policy Service field must be set to GTP or ANY to accept GTP-U packets.

The Carrier-enabled FortiGate unit intercepts packets with destination port 2152, removes the GTP header and handles the packets as regular IP packets. Applying an IPS sensor to the IP packets, the Carrier-enabled FortiGate unit can log attacks and pass or drop packets depending on the configuration of the sensor.

If the packet is GTP-in-GTP, or a nested tunnel, the packets are passed or blocked without being inspected.

To apply an IPS sensor to GTP-U tunnels

1. Go to **Security Profiles > Intrusion Protection > IPS Sensors** and select **Create New** to add an IPS Sensor.
2. Configure the IPS Sensor to detect attacks and log, drop, or pass attack packets.
   See the Intrusion Protection section of the FortiOS UTM Guide.
3. Go to **Policy & Objects > Policy > IPv4** and apply the IPS sensor to the security policy.
4. Go to **Policy & Objects > Policy > IPv4** and select Create New to add a security policy or select a security policy.
5. Configure the security policy to accept GTP traffic.
   In the security policy configure the source and destination settings to match the GTP traffic. Service to GTP or ANY so that the security policy accepts GTP traffic.
6. Select the GTP profile within the security policy.
7. Configure any other required security policy settings.
8. Select **OK** to save the security policy.

GTP packets are not moving along your network

When GTP packets are not getting to their destination, this could be caused by any one of a number of issues. General troubleshooting principals apply here.

The following sections provide some suggestions on how to troubleshoot this issue:

- Attempt to identify the section of your network with the problem
- Ensure you have an APN configured
- Check the logs and adjust their settings if required
- Check the routing table
- Perform a sniffer trace
- Generate specific packets to test the network

Attempt to identify the section of your network with the problem

The first step is to determine how widespread this problem is. Does it affect the whole GPRS network, or just one or two devices?

If the entire network is has this problem, the solution is likely a more general one such as ensuring the security policies allow GTP traffic to pass, the GTP profile specifies SSGNs and GSGNs, or ensuring the GTP general settings are not overly limiting.

If one part of the network is affected, the problem is more likely centered around configurations with those network devices specified such as the handover group, or authorized SGSNs/GGSNs. It is also possible that small portions of the network may have hardware related issues such as cabling or faulty hardware. This section does not address those issues, and assumes hardware is not the problem.

The handover group is a whitelist of GTP addresses allowed to handle GTP messages. If a device's address is not on this list, it will be denied.

Ensure you have an APN configured

When you configure your GTP profile, ensure you first configure the APN. Without it, there will be no flow of traffic. The APN is used in nearly all GTP communications and without it, the Carrier-enabled FortiGate unit doesn't have the information it needs.

Check the logs and adjust their settings if required

During normal operation, the log settings will show any problems on the network but may not provide the level of details required to fully troubleshoot the problem. The reason for this is that the level of detail required for troubleshooting would quickly overwhelm the daily logs without any real benefit.

GTP related events in the event log will have message IDs in the range 41216 to 41222. For more information on GTP log messages, see the Log Message Reference. For more information on logging in general, see the Logging and Reporting guide.

Once there is a problem to troubleshoot, check the logs to trace the traffic patterns and narrow down the possible sources of the problem. There may be enough detail for you to locate and fix the problem without changing the log settings.

Remember to set any changes you made to the log settings back to their original values when you are done troubleshooting. Otherwise, the amount of detail will overwhelm your logging.

However, if more detail is required you can change settings such as:

- Lower the Log Frequency number in GTP Profiles so fewer or no log messages are dropped. This will allow a more accurate picture of everything happening on the network, where you may have had only a partial picture before.
- Ensure all the GTP log events are enabled to provide you with a complete picture.
- Ensure that all relevant event types are enabled under **Log & Report > Log Config > Log Settings.**

For more information on GTP related logging, see Logging events on the Carrier-enabled FortiGate unit.

General information to look for in the logs includes:

- Are all packets having problems or just certain types?
- Are all devices on the network having problem, or just certain devices?
- Is it just GTP traffic that is having problems or are all types of traffic having the same problem?

Check the routing table

On any network, the routing table determines how packets reach their destination. This is also true on a carrier network.

If the Carrier-enabled FortiGate unit is running in NAT mode, verify that all desired routes are in the routing table — local subnets, default routes, specific static routes, and dynamic routing protocols. For complete information, it is best to check the routing table in the CLI. This method provides more complete information.

If VDOMs are enabled on your Carrier-enabled FortiGate unit, all routing related CLI commands must be performed within a VDOM and not in the global context.

To check the routing table using the CLI

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

S* 0.0.0.0/0 [10/0] via 192.168.183.254, port2
S 1.0.0.0/8 [10/0] via 192.168.183.254, port2
S 2.0.0.0/8 [10/0] via 192.168.183.254, port2
C 10.142.0.0/23 is directly connected, port3
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
C 192.168.182.0/23 is directly connected, port2
```

Examining an entry from the routing table above:

```
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
```

B	BGP. The routing protocol used.
10.160.0.0/23	The destination of this route including netmask.
[20/0]	20 indicates and administrative distance of 20 out of a range of 0 to 255. 0 is an additional metric associated with this route, such as in OSPF
10.142.0.74	The gateway, or next hop.
port3	The interface used by this route.
2d18h02m	How old this route is, in this case almost three days old.

Perform a sniffer trace

When troubleshooting network traffic, it helps to look inside the headers of packets to determine if they are traveling along the route you expect. Packet sniffing can also be called a network tap, packet capture, or logic analyzing.

If your Carrier-enabled FortiGate unit has NP interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP interfaces, disable offloading on those interfaces.

What can sniffing packets tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, what the port of entry is on the Carrier-enabled FortiGate unit, if the ARP resolution is correct, and if the traffic is being sent back to the source as expected.

Sniffing packets can also tell you if the Carrier-enabled FortiGate unit is silently dropping packets for reasons such as RPF (Reverse Path Forwarding), also called Anti Spoofing. This prevents an IP packet from being forwarded if its source IP address either does not belong to a locally attached subnet (local interface), or be a hop on the routing between the FortiOS Carrier and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymmetric enable`), however this will disable stateful inspection on the Carrier-enabled FortiGate unit and consequently cause many features to be turned off.

If you configure virtual IP addresses on your Carrier-enabled FortiGate unit, the unit will use those addresses in preference to the physical IP addresses. If not configured properly, secondary IP addresses can cause a broadcast storm. You will notice the secondary address being preferred when you are sniffing packets because all the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

How to sniff packets

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

<interface_name>	The name of the interface to sniff, such as `port1` or `internal`. This can also be `any` to sniff all interfaces.
<'filter'>	What to look for in the information the sniffer reads. `none` indicates no filtering, and all packets will be displayed as the other arguments indicate. The filter must be inside single quotes (‘).
<verbose>	The level of verbosity as one of: **1 -** print header of packets **2 -** print header and data from IP of packets **3 -** print header and data from Ethernet of packets
<count>	The number of packets the sniffer reads before stopping. If you don't put a number here, the sniffer will run forever unit you stop it with `<CTRL C>`.

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next 3 packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757

0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

Generate specific packets to test the network

If some packets are being delivered as expected while others are not, or after you believe you have fixed the problem, it is a good idea to generate specific traffic to test your network.

For example if you discover through log messages and packet sniffing that Create PDP Context Request messages are not being delivered between two SGSNs, you can generate those specific messages on your network to confirm they are the problem, and later that you have solved the problem and they are now being delivered as expected.

This step requires a third party traffic generation tool, either hardware or software. This is not be supported by Fortinet.

Chapter 7 - Compliance

Compliance

Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document discusses issues related to compliance, specifically Payment Card Industry Data Security Standard (PCI DSS).

This chapter contains the following topics:

- Before you begin
- How this guide is organized

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Configuring FortiGate units for PCI DSS compliance on page 793 explains the Payment Card Industry Data Security Standard (PCI DSS). It provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements.

Configuring FortiGate units for PCI DSS compliance

This chapter provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements. There is also some description of other Fortinet products that can help you with PCI DSS compliance.The following topics are included in this section:

- Introduction to PCI DSS
- Network topology
- Security policies for the CDE network
- Wireless network security
- Protecting stored cardholder data
- Protecting communicated cardholder data
- Protecting the CDE network from viruses
- Monitoring the network for vulnerabilities
- Restricting access to cardholder data
- Controlling access to the CDE network

Introduction to PCI DSS

The primary source of information for your PCI DSS compliance program is the Payment Card Industry (PCI) Data Security Standard itself. Version 3.0 of the standard was published in November 2013. The following is only a brief summary of PCI DSS.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) sets data handling requirements for organizations that hold, process, or exchange cardholder information.

What is the Cardholder Data Environment

Throughout the PCI DSS requirements, there are references to the Cardholder Data Environment (CDE). The CDE is the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.

PCI DSS objectives and requirements

PCI DSS consists of 7 control objectives and 12 requirements.

PCI DSS Control Objectives and Requirements

Control Objective	Requirement	Fortinet Solution
Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data	FortiGate firewall functionality. See Security policies for the CDE network.
	2. Do not use vendor - supplied defaults for system passwords and other security parameters	FortiDB vulnerability assessment and auditing FortiWeb web application password checking See Password complexity and change requirements.
Protect Cardholder Data	**3.** Protect stored cardholder data	FortiDB vulnerability assessment and monitoring FortiWeb web application firewall See Protecting stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks	FortiGate IPsec VPN. See Protecting communicated cardholder data.
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update antivirus software or programs	FortiGate integrated AV FortiClient integrated AV FortiMobile integrated AV FortiMail integrated AV FortiGuard automated AV updates See Protecting the CDE network from viruses.
	6. Develop and maintain secure systems and applications	FortiDB vulnerability assessment, auditing and monitoring FortiWeb web application security See Monitoring the network for vulnerabilities.

Control Objective	Requirement	Fortinet Solution
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need-to-know	FortiDB vulnerability assessment, auditing and monitoring. See Restricting access to cardholder data.
	8. Identify and authenticate access to system components	FortiGate integrated database or hooks to Active Directory. See Controlling access to the CDE network.
	9. Restrict physical access to cardholder data	Fortinet professional services in partnership with partner solutions
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data	FortiDB auditing and monitoring FortiAnalyzer event reporting See Monitoring the network for vulnerabilities.
	11. Regularly test security systems and processes	FortiDB vulnerability assessment See Monitoring the network for vulnerabilities.
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel	FortiManager security policy management appliance

This chapter describes how the FortiGate unit's features can help your organization to be compliant with PCI DSS. Requirements that the FortiGate cannot enforce need to be met through organization policies with some means determined for auditing compliance.

Be sure to read the section, Wireless guidelines, below. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

Wireless guidelines

While wired networks usually connect fixed known workstations, wireless networks are more dynamic, introducing a different set of security concerns.

Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that unauthorized wireless networking has not been introduced into the CDE. Wireless networking could be introduced quite casually by adding a wireless device to a PC on the CDE network.

For all PCI DSS networks, whether they use wireless technology or not, the following requirement applies:

- Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. (11.1)

If your organization uses wireless networking outside the CDE network and the firewall prevents communication with the CDE network, the wireless network is outside the PCI DSS scope, but the firewall configuration must meet PCI DSS requirements.

If your organization uses wireless networking inside the CDE network, the wireless network is within the PCI DSS scope. For information about wireless network requirements, see Wireless network security.

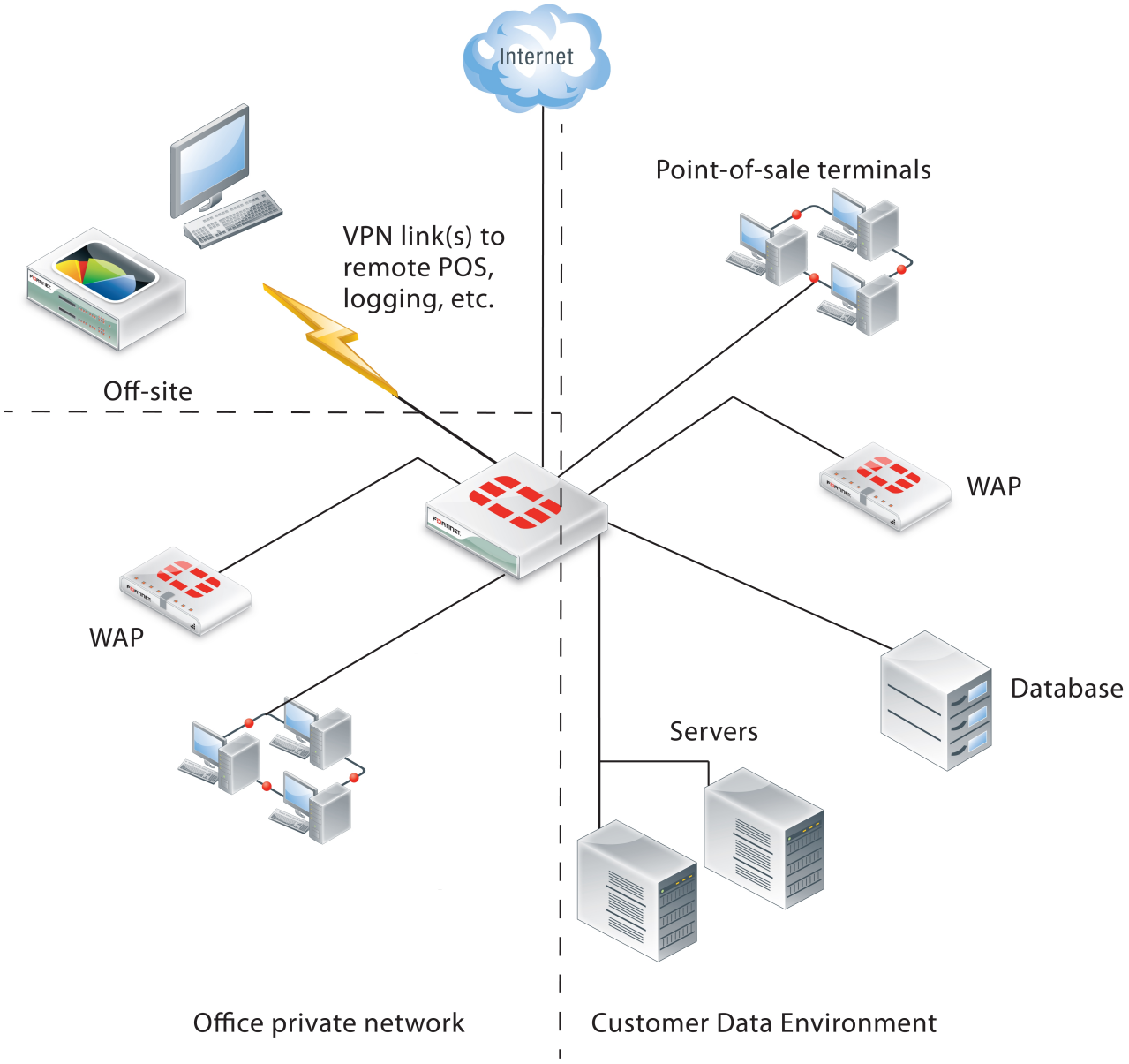
Network topology

The cardholder data environment must be protected against unauthorized access from the Internet and from other networks in your organization. FortiGate unit firewall functionality provides tight control over the traffic that can pass between the following network interfaces:

- Internet
- CDE wired LAN
- CDE wireless LAN
- Other internal networks

The figure below shows how the Cardholder Data Environment can be delineated in a typical network.

Enterprise network with a cardholder data environment



Internet

The FortiGate unit has at least one network interface connected to the Internet. If your organization uses more than one Internet service provider, there could be additional network interfaces that function as a route to the Internet.

The CDE wired LAN

The CDE network typically contains point-of-sale (POS) terminals, databases, and servers. The only security policies between the CDE network and the Internet should be for encrypted connections. For remote point-of-sale terminals or off-site databases, VPN connections are required and they should use strong encryption. For a web

server that handles online purchases, only HTTPS (SSL or TLS) connections can be permitted. The security policies that enable these connections should have the narrowest possible definitions for source address, destination address and service.

PCI DSS does not require the CDE network to be isolated from the rest of your corporate LAN. But isolating the CDE network reduces the scope of required data protection measures and may reduce the scope of PCI DSS assessments that are periodically required.

The CDE wireless LAN

Wireless networking is a special issue. Even if you do not use wireless technology you must monitor to ensure that unauthorized wireless access has not been added to the CDE network. For this purpose, the figure above shows a FortiAP device in the CDE. The FortiAP device can provide dedicated wireless monitoring, an access point, or both.

A small retail outlet could reduce costs by using a FortiWiFi unit, a FortiGate unit with integrated wireless networking. The FortiWiFi unit would have to be located where it could provide sufficient wireless monitoring (or access point) coverage for the entire premises.

Other internal networks

Other internal networks such as your office LAN, unless they provide connection to the CDE, are not subject to PCI DSS requirements.

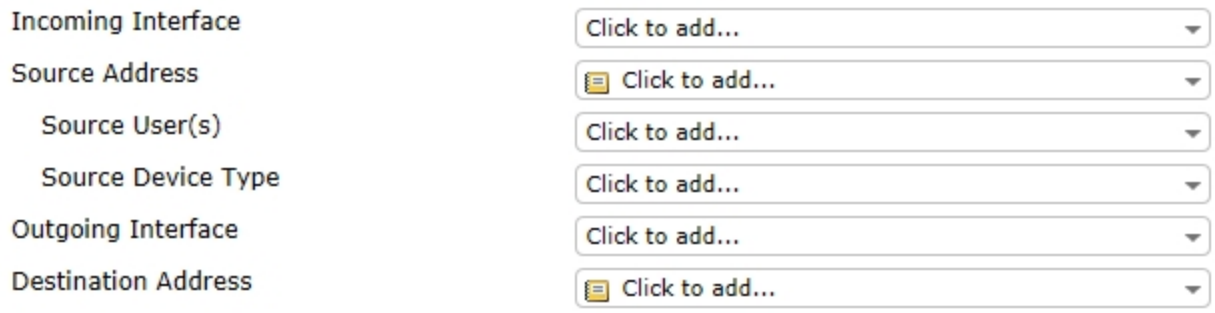
Security policies for the CDE network

The FortiGate unit's firewall functionality is ideally suited to PCI DSS requirement 1.2.1, "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." Security policies control the source, destination, and type of traffic passing between networks.

The PCI DSS standard includes requirements to document your network topology and configuration. As part of that requirement, and to assist the auditing of your network, make use of the **Comment** field available in FortiGate security policies. Describe the purpose of each policy.

Controlling the source and destination of traffic

The source and destination are the first parameters you specify in a security policy. (Go to **Policy & Objects > Policy > IPv4** and select **Create New**.)



The **Interface** settings depend on network topology. The **Address** settings define the IP addresses to which the policy applies. These should be as narrow as possible, so that only the appropriate hosts are included. For

example, if the destination is a server with a single IP address, the named Destination Address should be defined as that single address, not the entire subnet on which the server resides.

Addresses are defined in **Policy & Objects > Objects > Addresses**. You can also define a new address by selecting **Create** from either the **Source Address** or **Destination Address** drop-down lists in a security policy. Some addresses will be used in several security policies, so it is best to plan ahead and define the addresses first.

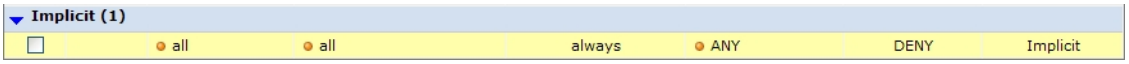
Controlling the types of traffic in the CDE

The **Service** setting in each security policy determines which types of traffic can pass based on protocol.

You can select a single protocol from the **Service** drop-down list. To add another protocol, select the green "+" button to access the **Service** drop-down list again. If several security policies will need the same list of services, consider creating a named service group. (Go to **Firewall Objects > Service > Groups**.) In the security policy, service groups are available at the bottom of the **Service** drop-down list.

The default deny policy

All traffic not specifically allowed by a security policy that you create is blocked by the Implicit policy listed at the bottom of the **Policy & Objects > Policy > IPv4** page.



You cannot delete this policy and you can edit the policy only to enable or disable logging of the traffic that it handles.

Wireless network security

Scanning for rogue access points is the minimum requirement for wireless security. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

If you use wireless networking, the wireless network is only within the PCI DSS scope if it can connect to the CDE.

On-wire detection of rogue APs

FortiGate units include an "on-wire" detection technique that correlates the SSID MAC addresses of the unknown access points with MAC addresses detected on your wired networks. This helps to differentiate unrelated neighboring APs from security-compromising unauthorized APs connected to your network.

Setting up rogue access point scanning

A FortiGate unit with a connected FortiAP unit can perform wireless scanning. Each of the FortiAP radios can act as a dedicated monitor or can perform scanning in the background while acting as a wireless access point.

Radio 1 operates in the 2.4GHz band and Radio 2 operates in the 5GHz band. Both bands should be monitored. The FortiAP unit(s) used for scanning must be located within the coverage area that would result if an access point were added to the CDE.

To configure rogue AP scanning in a FortiAP profile

1. Go to **WiFi Controller > WiFi Network > WIDS Profiles**.
   On some models, the menu is **WiFi & Switch Controller**.

2. Select an existing WIDS profile and edit it, or select **Create New**.
3. Make sure that **Enable Rogue AP Detection** is selected.
4. Select **Enable On-Wire Rogue AP Detection**.
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Select **OK**.

Viewing the results of rogue AP scanning

Go to **WiFi Controller > Monitor > Rogue AP Monitor** to view information about detected wireless access points.

Logging the results of rogue AP scanning

To ensure that detection of rogue access points is logged, go to **Log & Report > Log Config > Log Settings** and enable logging for **WiFi activity event**.

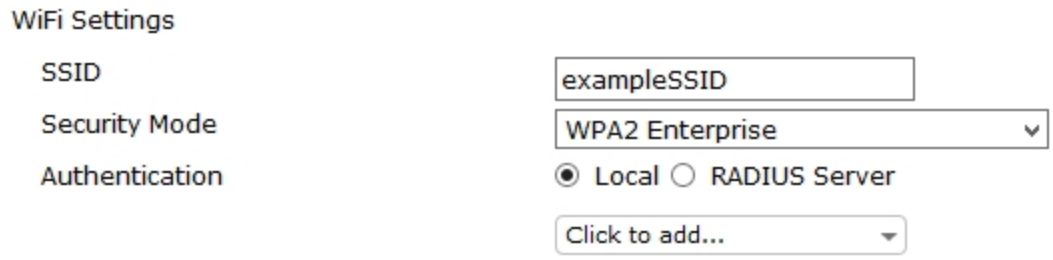
Securing a CDE network wireless access point

If your wireless network is within PCI DSS scope, it must meet the following requirements:

- Default settings such as SSID and passphrases must be changed.
- Use WPA/WPA2 security.
- Log wireless activity.

Setting wireless security

On FortiGate units, go to **WiFi Controller > WiFi Network > SSID** to configure wireless security settings for either a new or existing virtual access point.



The default SSID for the FortiAP is “fortinet”. You must change this.

The **Security Mode must** be set to one of the WPA/WPA2 modes. Both WPA or WPA2 clients can be served. In the CLI, you can optionally select exclusively WPA or WPA2 operation.

WPA/WPA2-Enterprise **Authentication** uses separate logon credentials for each user. Either FortiGate user group security or an external RADIUS server performs the authentication. Optionally, certificate-based security can also be applied. WPA/WPA2-Personal authentication requires a single pre-shared key that is used by all clients and is thus less secure.

For detailed information about wireless access points, see the Deploying Wireless Networks chapter of the FortiOS Handbook.

Logging wireless network activity

To ensure that wireless network activity is logged, go to **Log&Report > Log Config > Log Settings** and enable logging for **WiFi activity event**.

Protecting stored cardholder data

The Fortinet FortiDB and FortiWeb products can provide security for your sensitive cardholder data.

The Fortinet Database Security (FortiDB) device provides vulnerability assessment, database activity monitoring, auditing and monitoring. For more information about this product, see the Fortinet website, www.fortinet.com.

The Fortinet FortiWeb Web Application Firewall deployed in front of public-facing web applications protects Web applications, databases, and the information exchanged between them. In particular, it addresses the PCI DSS requirements 6.5 and 6.6 regarding web application vulnerabilities such as cross-site scripting, SQL injection, and information leakage. For more information about this product, see the Fortinet website, www.fortinet.com.

Protecting communicated cardholder data

If cardholder data must be communicated over an untrusted network, such as the Internet, use the FortiGate unit's IPsec VPN capability to exchange the data securely. If you support customer online transactions, use HTTPS (SSL or TLS encryption) for security. The relevant PCI DSS requirement is:

- Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. (4.1)

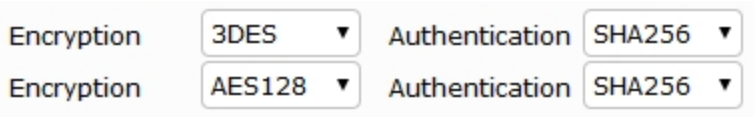
This does not prescribe particular cryptography, but it can be interpreted as a requirement to follow industry best practices.

Configuring IPsec VPN security

The security considerations for IPsec VPNs are encryption and authentication.

Encryption

Go to **VPN > IPsec > Tunnels** to configure an IPsec VPN. In both Phase 1 and Phase 2 parts of the configuration, you select the encryption to use.



These are advanced settings, overriding defaults that are not necessarily the strongest algorithms. VPNs negotiate over standards, so you can list multiple proposed algorithms. The VPN will use the strongest encryption that both ends support.

Choose strong encryption. The available encryption algorithms in descending order of strength are AES256, AES192, AES128, 3DES, DES. DES encryption is the weakest with only a 64-bit key and does not meet the 80-bit key length minimum that PCI DSS requires.

The message digest (authentication) algorithms in descending order of strength are SHA512, SHA384, SHA256, SHA1 and MD5. MD5 is particularly weak and should be avoided.

Authentication

VPN peers authenticate each other before establishing a tunnel. FortiGate units support two different authentication methods: pre-shared key and RSA signature (certificate). Certificates provide the best security. PCI DSS does not prohibit pre-shared keys, but you should limit access to the keys to the personnel who are responsible for the FortiGate units or other equipment at either end of the VPN.

Configuring SSL VPN security

The SSL VPN configuration includes a choice of encryption algorithm. You can only configure encryption key algorithms for SSL VPN in the CLI:

```
config vpn ssl settings
 set algorithm <low/medium/high>
end
```

The default option of **Medium** at **RC4 (128 bits)** is acceptable, but the **High** option, **AES (128/256 bits) and 3DES** is more secure. The **Low** option, **RC4 (64 bits), DES and higher** does not meet PCI DSS requirements.

Protecting the CDE network from viruses

PCI DSS requires the use of regularly updated antivirus protection. The antivirus functionality of the FortiGate unit protects both the FortiGate unit and the networks it manages. Workstations on these networks can be protected using FortiClient Endpoint Security. Both FortiGate and FortiClient antivirus protection can receive updates from Fortinet's FortiGuard service. Workstations can also use third-party antivirus applications with update services.

The FortiGate unit can enforce the use of antivirus software, denying unprotected workstations access to the network.

Enabling FortiGate antivirus protection

The antivirus profile must apply AV scanning to all protocols. You also need to enable SSL inspection to include secure protocols in antivirus scanning. The extended AV database contains the largest number of virus signatures.

To edit the antivirus profile

1. Go to **Security Profiles > AntiVirus**.
2. Edit the predefined profile or select **Create New**.
3. Set **Inspection Mode** to **Proxy**.
4. Ensure that all **Virus Scan and *Block*** check boxes are selected.
5. Select **Apply**.

To enable SSL inspection

1. Go to **Policy & Objects > Policy > SSL/SSH Inspection**.
   On some models, the option is **SSL Inspection**.
2. Set **Inspection Method** to **Full SSL Inspection**.
3. Set each listed protocol to **On** and then select **Apply**.

To select the extended antivirus database

The antivirus database is selectable using the CLI:

```
config antivirus settings
    set default-db extended
end
```

For detailed information about the Antivirus feature, see the Security Profiles chapter of the FortiOS Handbook.

Configuring antivirus updates

On the system dashboard, check the **License Information** widget. The **Support Contract** section should show Valid Contract and the contract expiry date. If your FortiGate unit is not registered, you need to visit the Fortinet Support web page (http://support.fortinet.com/) to register. Go to Product Registration and follow the instructions.

In the **FortiGuard Services** section, check the **Antivirus** field. If the service is unreachable, see the online Help for information about troubleshooting your connectivity to FortiGuard Services.

Enforcing firewall use on endpoint PCs

PCI DSS requires you to “install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. (1.4)” Consider using the Endpoint Control feature of the FortiGate unit to enforce use of this software.

Monitoring the network for vulnerabilities

There are several tools that can assist you in monitoring your network for vulnerabilities and provide evidence to the PCI DSS auditor of such monitoring.

FortiGate logs

FortiGate units can be configured to send logs to FortiAnalyzer unit. In a larger network, this enables you to collect log information in a central location from several FortiGate units.

Using the FortiOS Network Vulnerability Scan feature

As part of its security features, FortiGate units provide a Network Vulnerability Scan. You define assets to monitor, such as servers, workstations, or point-of-sale terminals. Then, the FortiGate unit scans those devices on a regular schedule. The scan checks TCP and UDP ports against a list of known vulnerabilities provided by FortiGuard Services. Scan settings determine how many of the ports are checked. Optionally, all ports are scanned.

Vulnerability scanning options in the web-based manager are now hidden by default. To enable vulnerability scanning, go to **System > Config > Features**, select **Show More**, turn on **Vulnerability Scan**, and select **Apply**.

To set up vulnerability scanning, go to **User & Device > Vulnerability Scan > Scan Definition**. To view scan logs, go to **User & Device > Vulnerability Scan > Vulnerability Result**. For more information, see Vulnerability Scan in the Managing Devices chapter of the FortiOS Handbook.

Monitoring with other Fortinet products

In addition to your FortiGate unit and its FortiOS firmware, there are several other Fortinet products that can assist your organization to comply with PCI DSS requirements.

Fortinet Database Security (FortiDB)

A FortiDB appliance or FortiDB software can provide vulnerability scanning and activity monitoring for your databases. For more information about this product, see the Fortinet website, www.fortinet.com.

FortiWeb Web Application Security

If your organization engages in e-Commerce, you can use FortiWeb Application Security to protect your web servers against attack. The FortiWeb application protects against HTTP and XML-based attacks, guards against attempts to deface your websites, and scans web servers for vulnerabilities. For more information about this product, see the Fortinet website, www.fortinet.com.

Restricting access to cardholder data

In addition to security policies and authentication governing access to the CDE, you can deploy the Fortinet Database Security (FortiDB) device, which provides vulnerability assessment, database activity monitoring, auditing and monitoring. For more information about this product, see the Fortinet website, www.fortinet.com.

Controlling access to the CDE network

PCI DSS requires each user to be uniquely identified and authenticated. On the FortiGate unit, this applies to administrators and to users of SSL VPN and IPsec VPNs.

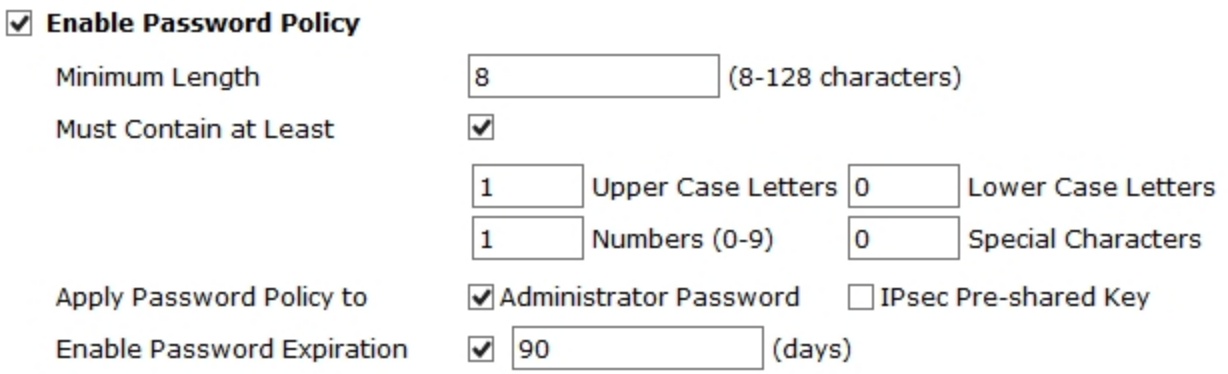
Password complexity and change requirements

By default, the FortiGate unit admin account has no password. Be sure to define a password.

PCI DSS password requirements are:

- Require a minimum length of at least seven characters. (8.2.3)
- Contain both numeric and alphabetic characters. (8.2.3)
- Change user passwords/passphrases at least every 90 days. (8.2.4)

To facilitate creation of compliant administrator passwords, you can set a password policy. Go to **System > Admin > Settings**. In the **Password Policy** section, enter the following and then select **Apply** at the bottom of the page.



Enable	Select the check box.
Minimum Length	8 or more. (Field does not accept a value less than 8.)
Must Contain	At minimum, set a required number of **Numerical Digits** and either **Upper Case Letters** or **Lower Case Letters**. Also setting a required number of **Non-alphabetic Letters** is acceptable.
Apply Password Policy to	Select **Administrator Password**.
Enable Password Expiration	Set to 90 days or less. The default is 90 days.

Note that the FortiGate password policy does not apply to user passwords. Both password complexity and password expiry for users would need to addressed by making them a policy in your organization.

Password non-reuse requirement

PCI DSS requires that passwords are not re-used to satisfy the change requirement:

- Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. (8.2.5)

FortiGate users don't set their own passwords. The super_admin administrators can and so can admins with appropriate access. There is, however, no FortiGate-based mechanism to enforce non re-use of passwords.

Administrator lockout requirement

PCI DSS requires a user account lockout for administrators to guard against unauthorized access attempts:

- Limit repeated access attempts by locking out the user ID after not more than six attempts. (8.1.6),
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.1.7)

You can meet these requirements with the following CLI commands:

```
config system global
     set admin-lockout-threshold 6
     set admin-lockout-duration 1800
    end
```

The threshold can be less than 6 and the lockout duration can be more than 1800.

Administrator timeout requirement

PCI DSS requires:

- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (8.1.8)

By default, the idle timeout is five minutes. You can go to **System > Admin > Settings** and change the **Idle Timeout** timeout to any value up to the permitted value of 15 minutes.

Administrator access security

To accommodate the requirement for unique identification of each user, the generic admin account should either be assigned to only one administrator or not used at all. You can create an administrator account for each administrator in **System > Admin > Administrators**.

If an administrator always works from the same workstation, consider using the Trusted Host feature. The administrator will be able to log in only from a trusted IP address. You can define up to three trusted IP addresses per administrator.

Administrative access must also be enabled per network interface. Go to **System > Network > Interface** to edit the interface settings. Enable administrative access only on interfaces where you would expect the administrator to connect. Allow only secure connection protocols, HTTPS for web-based access, SSH for CLI access.

Remote access security

For remote access, PCI DSS requires two-factor authentication: a password and some other authentication, such as a smart token or certificate. This applies to employees, administrators, and third parties.

SSL VPN users

For SSL VPN users, implement two-factor authentication by requiring users to have a certificate in addition to the correct password. Go to **VPN > SSL > Settings**, enable **Require Client Certificate**, and then select **Apply**. For more information, see the SSL VPN chapter of the FortiOS Handbook.

IPsec VPN users

If users access your network using an IPsec VPN, you can implement two-factor authentication by enabling extended authentication (XAUTH). This requires the user to enter a password in addition to the VPN authentication provided by the certificate or pre-shared key. As PCI DSS requires each user to have a unique identifier, you should already have user accounts and user groups defined.

To configure XAUTH on your VPN

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the Convert to Custom Tunnel button).
3. Under **XAuth**, select the **Server Type** setting, which determines the type of encryption method to use between the XAuth client, the FortiGate unit and the authentication server. Select one of the following options:
   - **PAP Server** —Password Authentication Protocol.
   - **CHAP Server** — Challenge-Handshake Authentication Protocol.

- **Auto Server** —Use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server. This option allows multiple source interfaces to be defined in an IPsec/IKE policy.

4. From the **User Group** list, select the user group that needs to access the private network behind the FortiGate unit. The group must be added to the FortiGate configuration before it can be selected here. For multiple source interfaces to be defined in the IPsec/IKE policy, select **Inherit Groups from Policy**.
5. Select **OK**.

Chapter 8 - Deploying Wireless Networks

This FortiOS Handbook chapter contains the following sections:

Introduction to wireless networking explains the basic concepts of wireless networking and how to plan your wireless network.

Configuring a WiFi LAN explains how to set up a basic wireless network, prior to deploying access point hardware.

Access point deployment explains how to deploy access point hardware and add it to your wireless network configuration.

Wireless Mesh explains how to configure a Wi-Fi network where access points are connected to the Wi-Fi controller wirelessly instead of by Ethernet.

Combining WiFi and wired networks with a software switch shows how to use the FortiAP Wi-Fi-Ethernet bridge feature.

Protecting the WiFi Network explains the Wireless Intrusion Detection System (WIDS).

Wireless network monitoring explains how to monitor your wireless clients and how to monitor other wireless access points, potentially rogues, in your coverage area.

Configuring wireless network clients explains how to configure typical wireless clients to work with a WPA-Enterprise protected network.

Wireless network examples provides two examples. The first is a simple Wi-Fi network using automatic configuration. The second is a more complex example of a business with two Wi-Fi networks, one for employees and another for guests or customers.

Using a FortiWiFi unit as a client explains how to use a FortiWiFi unit as a wireless client to connect to other Wi-Fi networks. This connection can take the place of an Ethernet connection where wired access to a network or to the Internet is not available.

Support for location-based services explains how Fortinet supports location-based services that collect information about devices near FortiGate-managed access points, even if the devices don't associate with the network.

Reference provides information about Wi-Fi radio channels.

Introduction to wireless networking

This chapter introduces some concepts you should understand before working with wireless networks, describes Fortinet's wireless equipment, and then describes the factors you need to consider in planning deployment of a wireless network.

Wireless concepts
Security
Authentication
Wireless networking equipment
Automatic Radio Resource Provisioning

Wireless concepts

Wireless networking is radio technology, subject to the same characteristics and limitations as the familiar audio and video radio communications. Various techniques are used to modulate the radio signal with a data stream.

Bands and channels

Depending on the wireless protocol selected, you have specific channels available to you, depending on what region of the world you are in.

- IEEE 802.11b and g protocols provide up to 14 channels in the 2.400-2.500 GHz Industrial, Scientific and Medical (ISM) band.
- IEEE 802.11a,n (5.150-5.250, 5.250-5.350, 5.725–5.875 GHz, up to 16 channels) in portions of Unlicensed National Information Infrastructure (U-NII) band

Note that the width of these channels exceeds the spacing between the channels. This means that there is some overlap, creating the possibility of interference from adjacent channels, although less severe than interference on the same channel. Truly non-overlapping operation requires the use of every fourth or fifth channel, for example ISM channels 1, 6 and 11.

The capabilities of your wireless clients is the deciding factor in your choice of wireless protocol. If your clients support it, 5GHz protocols have some advantages. The 5GHz band is less used than 2.4GHz and its shorter wavelengths have a shorter range and penetrate obstacles less. All of these factors mean less interference from other access points, including your own.

When configuring your WAP, be sure to correctly select the Geography setting to ensure that you have access only to the channels permitted for WiFi use in your part of the world.

For detailed information about the channel assignments for wireless networks for each supported wireless protocol, see Reference on page 913.

Power

Wireless LANs operate on frequencies that require no license but are limited by regulations to low power. As with other unlicensed radio operations, the regulations provide no protection against interference from other users who are in compliance with the regulations.

Power is often quoted in dBm. This is the power level in decibels compared to one milliwatt. 0dBm is one milliwatt, 10dBm is 10 milliwatts, 27dBm, the maximum power on Fortinet FortiAP equipment, is 500 milliwatts. The FortiGate unit limits the actual power available to the maximum permitted in your region as selected by the WiFi controller country setting.

Received signal strength is almost always quoted in dBm because the received power is very small. The numbers are negative because they are less than the one milliwatt reference. A received signal strength of -60dBm is one millionth of a milliwatt or one nanowatt.

Antennas

Transmitted signal strength is a function of transmitter power and antenna gain. Directional antennas concentrate the signal in one direction, providing a stronger signal in that direction than would an omnidirectional antenna.

FortiWiFi units have detachable antennas. However, these units receive regulatory approvals based on the supplied antenna. Changing the antenna might cause your unit to violate radio regulations.

Security

There are several security issues to consider when setting up a wireless network.

Whether to broadcast SSID

It is highly recommended to broadcast the SSID. This makes connection to a wireless network easier because most wireless client applications present the user with a list of network SSIDs currently being received. This is desirable for a public network.

Attempting to obscure the presence of a wireless network by not broadcasting the SSID does not improve network security. The network is still detectable with wireless network “sniffer” software. Clients search for SSIDs that they know, leaking the SSID. Refer to RFC 3370. Also, many of the latest Broadcom drivers do not support hidden SSID for WPA2.

Encryption

Wireless networking supports the following security modes for protecting wireless communication, listed in order of increasing security.

None — Open system. Any wireless user can connect to the wireless network.

WEP64 — 64-bit Web Equivalent Privacy (WEP). This encryption requires a key containing 10 hexadecimal digits.

WEP128 — 128-bit WEP. This encryption requires a key containing 26 hexadecimal digits.

WPA — 256-bit WiFi Protected Access (WPA) security. This encryption can use either the TKIP or AES encryption algorithm and requires a key of either 64 hexadecimal digits or a text phrase of 8 to 63 characters. It is also possible to use a RADIUS server to store a separate key for each user.

WPA2 — WPA with security improvements fully meeting the requirements of the IEEE 802.11i standard. Configuration requirements are the same as for WPA.

For best security use the WPA2 with AES encryption and a RADIUS server to verify individual credentials for each user. WEP, while better than no security at all, is an older algorithm that is easily compromised. With either WEP or WAP, changing encryption passphrases on a regular basis further enhances security.

Separate access for employees and guests

Wireless access for guests or customers should be separate from wireless access for your employees. This does not require additional hardware. Both FortiWiFi units and FortiAP units support multiple wireless LANs on the same access point. Each of the two networks can have its own SSID, security settings, firewall policies, and user authentication.

A good practice is to broadcast the SSID for the guest network to make it easily visible to users, but not to broadcast the SSID for the employee network.

Two separate wireless networks are possible because multiple virtual APs can be associated with an AP profile. The same physical APs can provide two or more virtual WLANs.

Captive portal

As part of authenticating your users, you might want them to view a web page containing your acceptable use policy or other information. This is called a captive portal. No matter what URL the user initially requested, the portal page is returned. Only after authenticating and agreeing to usage terms can the user access other web resources.

For more information about captive portals, see the Captive portals chapter of the FortiOS Authentication Guide.

Power

Reducing power reduces unwanted coverage and potential interference to other WLANs. Areas of unwanted coverage are a potential security risk. There are people who look for wireless networks and attempt to access them. If your office WLAN is receivable out on the public street, you have created an opportunity for this sort of activity.

Monitoring for rogue APs

It is likely that there are APs available in your location that are not part of your network. Most of these APs belong to neighboring businesses or homes. They may cause some interference, but they are not a security threat. There is a risk that people in your organization could connect unsecured WiFi-equipped devices to your wired network, inadvertently providing access to unauthorized parties. The optional On-Wire Rogue AP Detection Technique compares MAC addresses in the traffic of suspected rogues with the MAC addresses on your network. If wireless traffic to non-Fortinet APs is also seen on the wired network, the AP is a rogue, not an unrelated AP.

Decisions about which APs are rogues are made manually on the Rogue AP monitor page. For detailed information, see Wireless network monitoring on page 870.

Suppressing rogue APs

When you have declared an AP to be a rogue, you have the option of suppressing it. To suppress and AP, the FortiGate WiFi controller sends reset packets to the rogue AP. Also, the MAC address of the rogue AP is blocked in the firewall policy. You select the suppression action on the Rogue AP monitor page. For more information, see Wireless network monitoring on page 870.

Rogue suppression is available only when there is a radio dedicated to scanning. It will not function during background scanning for spectrum analysis.

Wireless Intrusion Detection (WIDS)

You can create a WIDS profile to enable several types of intrusion detection:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking

For more information, see Protecting the WiFi Network on page 867.

Authentication

Wireless networks usually require authenticated access. FortiOS authentication methods apply to wireless networks the same as they do to wired networks because authentication is applied in the firewall policy.

The types of authentication that you might consider include:

- user accounts stored on the FortiGate unit
- user accounts managed and verified on an external RADIUS, LDAP or TACACS+ server
- Windows Active Directory authentication, in which users logged on to a Windows network are transparently authenticated to use the wireless network.

This Wireless chapter of the FortiOS Handbook will provide some information about each type of authentication, but more detailed information is available in the Authentication chapter.

What all of these types of authentication have in common is the use of user groups to specify who is authorized. For each wireless LAN, you will create a user group and add to it the users who can use the WLAN. In the identity-based firewall policies that you create for your wireless LAN, you will specify this user group.

Some access points, including FortiWiFi units, support MAC address filtering. You should not rely on this alone for authentication. MAC addresses can be “sniffed” from wireless traffic and used to impersonate legitimate clients.

Wireless networking equipment

Fortinet produces two types of wireless networking equipment:

- FortiWiFi units, which are FortiGate units with a built-in wireless access point/client
- FortiAP units, which are wireless access points that you can control from any FortiGate unit that supports the WiFi Controller feature.

FortiWiFi units

A FortiWiFi unit can:

- Provide an access point for clients with wireless network cards. This is called Access Point mode, which is the default mode.

or

- Connect the FortiWiFi unit to another wireless network. This is called Client mode. A FortiWiFi unit operating in client mode can only have one wireless interface.

or

- Monitor access points within radio range. This is called Monitoring mode. You can designate the detected access points as Accepted or Rogue for tracking purposes. No access point or client operation is possible in this mode. But, you can enable monitoring as a background activity while the unit is in Access Point mode.

The Products section of the Fortinet web site (www.fortinet.com) provides detailed information about the FortiWiFi models that are currently available.

FortiAP units

FortiAP units are thin wireless access points are controlled by either a FortiGate unit or FortiCloud service.

FortiAP is a family of Indoor, Outdoor and Remote Access Point models supporting the latest single, dual, and triple stream MIMO 802.11ac and 802.11n technology, as well as 802.11g and 802.11a.

For large deployments, some FortiAP models support a mesh mode of operation in which control and data backhaul traffic between APs and the controller are carried on a dedicated WiFi network. Users can roam seamlessly from one AP to another.

In dual-radio models, each radio can function as an AP or as a dedicated monitor. The monitoring function is also available during AP operation, subject to traffic levels.

The Products section of the Fortinet web site (www.fortinet.com) provides detailed information about the FortiAP models that are currently available.

Automatic Radio Resource Provisioning

To prevent interference between APs, the FortiOS WiFi Controller includes the Automatic Radio Resource Provisioning (ARRP) feature. When enabled in an access point profile, **Radio Resource Provision** measures utilization and interference on the available channels and selects the clearest channel at each access point. The measurement can be repeated periodically to respond to changing conditions.

Configuring a WiFi LAN

When working with a FortiGate WiFi controller, you can configure your wireless network before you install any access points. If you are working with a standalone FortiWiFi unit, the access point hardware is already present but the configuration is quite similar. Both are covered in this section.

Overview of WiFi controller configuration
Setting your geographic location
Creating a FortiAP Profile
Defining a wireless network interface (SSID)
Dynamic VLAN assignment
Configuring user authentication
Configuring firewall policies for the SSID
Configuring the built-in access point on a FortiWiFi unit

On FortiGate model 30D, web-based manager configuration of the WiFi controller is disabled by default. To enable it, enter the following CLI commands:

```
config system global
  set gui-wireless-controller enable
end
```

If you want to connect and authorize external APs, such as FortiAP units, see the next chapter, Access point deployment.

Overview of WiFi controller configuration

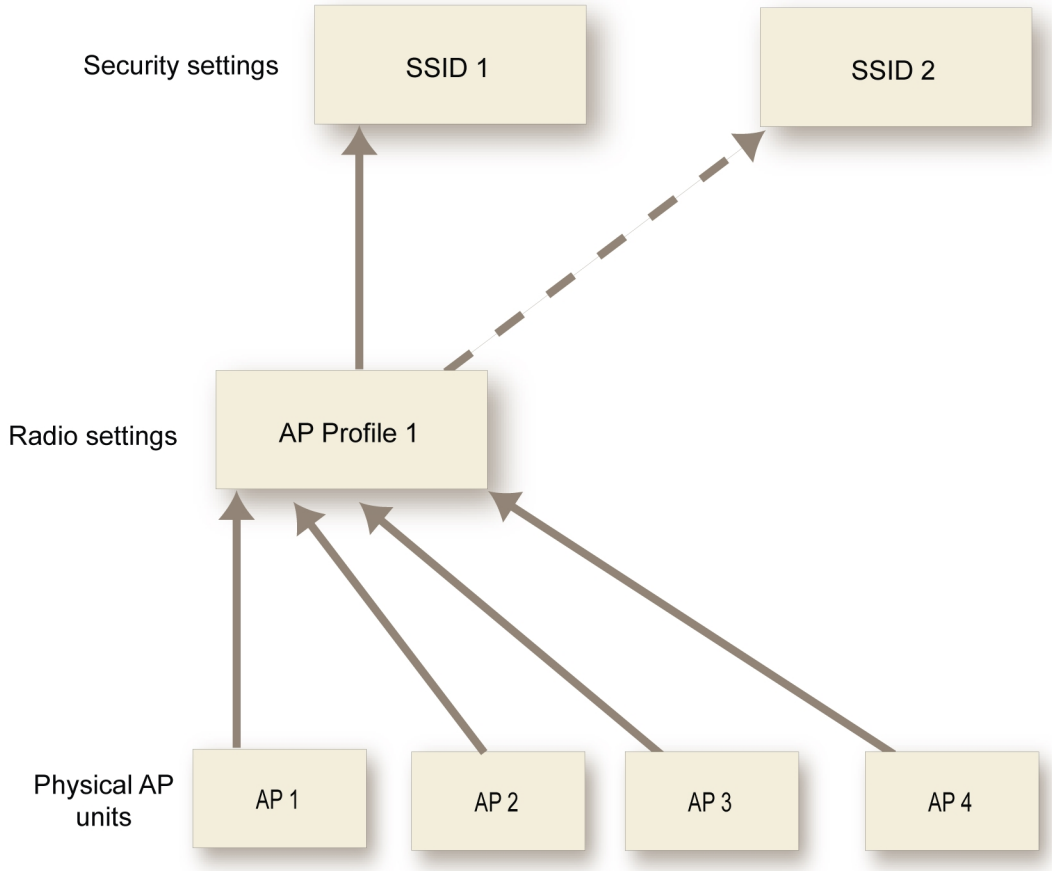
The FortiGate WiFi controller configuration is composed of three types of object, the SSID, the AP Profile and the physical Access Point.

- An **SSID** defines a virtual wireless network interface, including security settings. One SSID is sufficient for a wireless network, regardless how many physical access points are provided. You might, however, want to create multiple SSIDs to provide different services or privileges to different groups of users. Each SSID has separate firewall policies and authentication. Each radio in an access point can support up to 8 SSIDs.

A more common use of the term SSID is for the identifier that clients must use to connect to the wireless network. Each SSID (wireless interface) that you configure will have an SSID field for this identifier. In Managed Access Point configurations you choose wireless networks by SSID values. In firewall policies you choose wireless interfaces by their SSID name.

- An **AP Profile** defines the radio settings, such as band (802.11g for example) and channel selection. The AP Profile names the SSIDs to which it applies. Managed APs can use automatic profile settings or you can create AP profiles.
- **Managed Access Points** represent local wireless APs on FortiWiFi units and FortiAP units that the FortiGate unit has discovered. There is one managed access point definition for each AP device. An access point definition can use automatic AP profile settings or select a FortiAP Profile. When automatic profile settings are used, the managed AP definition also selects the SSIDs to be carried on the AP.

Conceptual view of FortiGate WiFi controller configuration



About SSIDs on FortiWiFi units

FortiWiFi units have a default SSID (wireless interface) named **wlan.** You can modify or delete this SSID as needed. As with external APs, the built-in wireless AP can be configured to carry any SSID.

The AP settings for the built-in wireless access point are located at **WiFi Controller > Managed Access Points > Local WiFi Radio**. The available operational settings are the same as those for external access points which are configured at **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Process to create a wireless network

To set up your wireless network, you will need to perform the following steps:

- Make sure the FortiGate wireless controller is configured for your geographic location. This ensures that the available radio channels and radio power are in compliance with the regulations in your region.
- Optionally, if you don't want to use automatic AP profile settings, configure a FortiAP profile, specifying the radio settings and the SSIDs to which they apply.
- Configure one or more SSIDs for your wireless network. The SSID configuration includes DHCP and DNS settings.
- Configure the user group and users for authentication on the WLAN.

- Configure the firewall policy for the WLAN.
- Optionally, customize the captive portal.
- Configure access points.
  Configuration of the built-in AP on FortiWiFi units is described in this chapter. Connection and configuration of FortiAP units is described in the next chapter, see Access point deployment on page 834.

Setting your geographic location

The maximum allowed transmitter power and permitted radio channels for WiFi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, you need to set your location before you begin configuring wireless networks.

To change the location setting - CLI

To change the country to France, for example, enter

```
config wireless-controller setting
   set country FR
end
```

To see the list of country codes, enter a question mark ('?') instead of a country code.

Before changing the country setting, you must remove all FortiAP Profiles. To do this, go to **WiFi Controller > WiFi Network > FortiAP Profiles**.

Creating a FortiAP Profile

A FortiAP Profile defines radio settings for a particular platform (FortiAP model). The profile also selects which SSIDs (virtual APs) the APs will carry. FortiAP units contain two radio transceivers, making it possible, for example, to provide both 2.4GHz 802.11b/g/n and 5GHz 802.11a/n service from the same access point. The radios can also be used for monitoring, used for the Rogue AP detection feature.

You can modify existing FortiAP profiles or create new ones of your own.

On FortiGate model 30D, web-based manager configuration of FortiAP Profiles is disabled by default. To enable AP profiles, enter the following CLI commands:

```
config system global
  set gui-ap-profile enable
end
```

To configure a FortiAP Profile - web-based manager

1. Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and select **Create New**.
2. Enter a **Name** for the FortiAP Profile.
3. In **Platform**, select the FortiWiFi or FortiAP model to which this profile applies.
4. For each radio, enter:

Mode	Select the type of mode. **Disable** – radio disabled **Access Point** – the platform is an access point **Dedicated Monitor** – the platform is a dedicated monitor. See Wireless network monitoring on page 870.
Spectrum Analysis	Select to enable monitoring other APs in the background, even while operating as an AP. By default, spectrum analsis is disabled. See Wireless network monitoring on page 870.
WIDS Profile	Optionally, select a Wireless Intrusion Detection (WIDS) profile. See Protecting the WiFi Network on page 867.
Radio Resource Provision	Select to enable the radio resource provision feature. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point. The measurement can be repeated periodically to respond to changing conditions.
Client Load Balancing	Select Frequency Handoff or AP Handoff as needed. See Access point deployment on page 834.
Band	Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11bg" means 802.11b **and** 802.11g. For 802.11n, 802.11n_2.4G indicates 2.4GHz, 802.11n_5G indicates 5GHz. Note that on two-radio units such as the FortiAP-220B it is not possible to put both radios on the same band.
Select Channel Width	Select to enable 20MHz or 40MHz channel width for 802.11n-5G.
Short Guard Interval	Select to enable the short guard interval for 802.11n_5G with 40MHz channel width.
Channel	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in **Band**. By default, all available channels are enabled.
Auto Tx Power Control	Optionally, enable automatic adjustment of transmit power, specifying minimum and maximum power levels.
TX Power	By default, the TX power is set to 100% of the maximum power permitted in your region. To change the level, drag the slider.
SSID	Choose the SSIDs (WiFi networks) that APs using this profile will carry.

Radio 1 settings are the same as Radio 2 settings except for the options for **Channel**.
Radio 2 settings are available only for FortiAP models with dual radios.

5. Select **OK**.

To configure a FortiAP Profile - CLI

This example configures a FortiAP-220B to use only Radio 2 for 802.11g operation applied to SSID example_wlan.

```
config wireless-controller wtp-profile
   edit guest_prof
      config platform
         set type 220B
      end
      config radio-2
         set mode ap
         set band 802.11g
         set vaps example_wlan
      end
   end
```

Defining a wireless network interface (SSID)

You begin configuring your wireless network by defining one or more SSIDs to which your users will connect. When you create an SSID, a virtual network interface is also created with the **Name** you specified in the SSID configuration. You can configure the settings of an existing SSID in either **WiFi Controller > WiFi Network > SSID** or **System > Network > Interface**.

To create a new SSID

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Fill in the SSID fields as described below.

To configure the settings of an existing SSID

1. Either
   - Go to **WiFi Controller > WiFi Network > SSID**.

   or

   - Go to **System > Network > Interfaces**.
     WiFi interfaces list the SSID beside the interface **Name**.
2. Edit a WiFi interface, modifying the SSID fields as needed.

SSID fields

Interface Name	Enter a name for the SSID interface.
Type	WiFi SSID.
Traffic Mode	**Tunnel to Wireless Controller** — Data for WLAN passes through WiFi Controller. This is the default. **Local bridge with FortiAP's Interface** — FortiAP unit Ethernet and WiFi interfaces are bridged. **Mesh Downlink** — Radio receives data for WLAN from mesh backhaul SSID.
IP/Network Mask	Enter the IP address and netmask for the SSID.
IPv6 Address	Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.
Administrative Access	Select which types of administrative access are permitted on this SSID.
IPv6 Administrative Access	If you have IPv6 addresses, select the permitted IPv6 administrative access types for this SSID.
DHCP Server	Select **Enable** to enable a DHCP server and define IP address ranges to assign to clients or to relay DHCP requests to another server. If the unit is in transparent mode, the DHCP server settings will be unavailable. For more information, see Configuring DHCP for WiFi clients on page 823.
WiFi Settings	
SSID	Enter the SSID. By default, this field contains `fortinet`.
Security Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. Additional security mode options are available in the CLI. For more information, see Configuring security on page 824.
	Captive Portal – authenticates users through a customizable web page.
	WPA2-Personal – WPA2 is WiFi Protected Access version 2. There is one pre-shared key (password) that all users use.
	WPA2-Personal with Captive Portal – The user will need to know the pre-shared key and will also be authenticated through the custom portal.
	WPA2-Enterprise – similar to WPA2-Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password.

Pre-shared Key	Available only when **Security Mode** is **WPA2-Personal**. Enter the encryption key that the clients must use.
Authentication	Available only when **Security Mode** is **WPA2-Enterprise**. Select one of the following: **RADIUS Server** — Select the RADIUS server that will authenticate the clients. **Usergroup** – Select the user group(s) that can authenticate.
Portal Type	Available only when **Security Mode** is **Captive Portal**. Choose the captive portal type. Authentication is available with or without a usage policy disclaimer notice.
Authentication Portal	**Local** - portal hosted on the FortiGate unit **Remote** - enter FQDN or IP address of external portal
User Groups	Select permitted user groups.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Click the listed portal pages to edit them.
User Groups	Available only when **Security Mode** is **Captive Portal**. Select the user groups that can authenticate. To select a user group, select the group in **Available** and then use the -> arrow to move that group to **Selected**. To remove a user group from **Selected**, select the group and then use the <- arrow to move the group back to **Available**.
Redirect after Captive Portal	Optionally, select **Specific URL** and enter a URL for user redirection after captive portal authentication. By default, users are redirected to the URL that they originally requested.
Allow New WiFi Client Connections When Controller Is Down	This option is available for local bridge SSIDs with WPA-Personal security. See Combining WiFi and wired networks with a software switch on page 855.
Broadcast SSID	Optionally, disable broadcast of SSID. By default, the SSID is broadcast. For more information, see Introduction to wireless networking on page 810.
Block Intra-SSID Traffic	Select to enable the unit to block intra-SSID traffic.
Maximum Clients	Select to limit the number of clients permitted to connect simultaneously. Enter the limit value.

Split Tunneling	Select to enable some subnets to remain local to the remote FortiAP. Traffic for these networks is not routed through the WiFi Controller. Specify split-tunnel networks in the FortAP Profile. See Split tunneling on page 861.
Optional VLAN ID	Enter the ID of the VLAN this SSID belongs to. Enter 0 for non-VLAN operation.
Device Management	Select **Detect and Identify Devices** if you want to monitor the device types using this interface or create device identity policies involving this interface. Optionally, enable **Add New Devices to Vulnerability Scan List**.
Enable Explicit Web Proxy	Select to enable explicit web proxy for the SSID.
Listen for RADIUS Accounting Messages	Enable if you are using RADIUS-based Single Sign-On (SSO).
Secondary IP Address	Optioanally, enable and define secondary IP addresses. Administrative access can be enabled on secondary interfaces.
Comments	Enter a description or comment for the SSID.

To configure a virtual access point (SSID) - CLI

This example creates an access point with SSID “example” and WPA2-Personal security. The wireless interface is named example_wlan.

```
config wireless-controller vap
   edit example_wlan
      set ssid "example"
      set broadcast-ssid enable
      set security wpa2-only-personal
      set passphrase "hardtoguess”
      set vdom root
   end
config system interface
   edit example_wlan
      set ip 10.10.120.1 255.255.255.0
   end
```

Configuring DHCP for WiFi clients

Wireless clients need to have IP addresses. If you use RADIUS authentication, each user’s IP address can be stored in the Framed-IP-Address attribute. Otherwise, you need to configure a DHCP server on the WLAN interface to assign IP addresses to wireless clients.

To configure a DHCP server for WiFi clients - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and edit your SSID entry.
2. In **DHCP Server** select **Enable**.
3. In **Address Range**, select **Create New**.

4. In the **Starting IP** and **End IP** fields, enter the IP address range to assign.
   The address range needs to be in the same subnet as the wireless interface IP address, but not include that address.
5. Set the **Netmask** to an appropriate value, such as 255.255.255.0.
6. Set the **Default Gateway** to **Same as Interface IP**.
7. Set the **DNS Server** to **Same as System DNS**.
8. If you want to restrict access to the wireless network by MAC address, see "Defining a wireless network interface (SSID)" on page 826.
9. Select **OK**.

To configure a DHCP server for WiFi clients - CLI

In this example, WiFi clients on the example_wlan interface are assigned addresses in the 10.10.120.2-9 range to connect with the WiFi access point on 10.10.120.1.

```
config system dhcp server
   edit 0
      set default-gateway 10.10.120.1
      set dns-service default
      set interface example_wlan
      set netmask 255.255.255.0
      config ip-range
         edit 1
            set end-ip 10.10.120.9
            set start-ip 10.10.120.2
         end
      end
```

You cannot delete an SSID (wireless interface) that has DHCP enabled on it.

Configuring security

Using the web-based manager, you can configure Captive Portal security or WiFi Protected Access version 2 (WPA2) security modes WPA2-Personal and WPA2-Enterprise. Using the CLI, you can also choose WPA/WPA2 modes that support both WPA version 1 and WPA version 2.

WPA2 security with a pre-shared key for authentication is called WPA2-Personal. This can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

A more secure form of WPA2 security is WPA2-Enterprise. Users each have their own authentication credentials, verified through an authentication server, usually RADIUS. FortiOS can also authenticate WPA2-Enterprise users through its built-in user group functionality. FortiGate user groups can include RADIUS servers and can select users by RADIUS user group. This makes possible Role-Based Access Control (RBAC).

By default, WPA2 security encrypts communication using Advanced Encryption Standard (AES). But some older wireless clients support only Temporal Key Integrity Protocol (TKIP) . You can change the encryption to TKIP or negotiable TKIP-AES in the CLI. For example, to accomodate clients with either TKIP or AES, enter:

```
config wireless-controller vap
   edit example_wlan
      set security wpa-personal
```

```
      set passphrase "hardtoguess"
      set encrypt TKIP-AES
   end
```

Captive Portal security connects users to an open web portal defined in replacement messages. To navigate to any location beyond the web portal, the user must pass FortiGate user authentication.

WPA-Personal security

WPA2-Personal security setup requires only the preshared key that you will provide to your clients.

To configure WPA2-Personal security - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Personal**.
3. In **Pre-shared Key**, enter a key between 8 and 63 characters long.
4. Select **OK**.

To configure WPA2-Personal security - CLI

```
config wireless-controller vap
   edit example_wlan
      set security wpa2-personal
      set passphrase "hardtoguess"
   end
```

WPA-Enterprise security

If you will use FortiOS user groups for authentication, go to **User & Device > User > User Groups** and create those groups first. The groups should be Firewall groups.

If you will use a RADIUS server to authenticate wireless clients, you must first configure the FortiGate unit to access the RADIUS server.

To configure FortiGate unit access to the RADIUS server - web-based manager

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.
3. In **Primary Server Name/IP**, enter the network name or IP address for the server.
4. In **Primary Server Secret**, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select **OK**.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
   edit exampleRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret aoewmntiasf
   end
```

To configure WPA-Enterprise security - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Enterprise**.
3. In **Authentication**, do one of the following:
   - If you will use a RADIUS server for authentication, select **RADIUS** Server and then select the RADIUS server.
   - If you will use a local user group for authentication, select **Local** and then select the user group(s) permitted to use the wireless network.
4. Select **OK**.

To configure WPA-Enterprise security - CLI

```
config wireless-controller vap
   edit example_wlan
      set security wpa2-enterprise
      set auth radius
      set radius-server exampleRADIUS
   end
```

Captive Portal security

Captive Portal security provides an access point that initially appears open. The wireless client can connect to the AP with no security credentials. The AP responds to the client's first HTTP request with a web page requesting user name and password. Until the user enters valid credentials, no communication beyond the AP is permitted.

For more information about captive portals, see the Captive Portal chapter of the Authentication Guide.

Adding a MAC filter

On each SSID, you can create a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.

This is actually not as secure as it appears. Someone seeking unauthorized access to your network can obtain MAC addresses from wireless traffic and use them to impersonate legitimate users. A MAC filter list should only be used in conjunction with other security measures such as encryption.

To configure a MAC filter - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and edit your SSID entry.
2. In the **DHCP Server** section, expand **Advanced**.
3. In **MAC Reservation + Access Control**, double-click in the **Unknown MAC Addresses** line and select **Assign IP** or **Block**, as needed.
   By default, unlisted MAC addresses are assigned an IP address automatically.
4. In **MAC Reservation + Access Control**, select **Create New**.
5. Enter a MAC address In the **MAC** field.
6. In **IP or Action**, select one of:
   - **Reserve IP** — enter the IP address that is always assigned to this MAC address.
   - **Assign IP —** an IP address is assigned to this MAC address automatically.
   - **Block** — This MAC address will not be assigned an IP address.

7. Repeat steps 4 through 6 for each additional MAC address that you want to add.
8. Select **OK**.

To configure a MAC filter - CLI

1. Enter
```
config system dhcp server
show
```
2. Find the entry where `interface` is your WiFi interface. Edit that entry and configure the MAC filter. In this example, the MAC address 11:11:11:11:11:11will be excluded. Unlisted MAC addresses will be assigned an IP address automatically.
```
edit 3
   config reserved-address
      edit 1
         set action block
         set mac 11:11:11:11:11:11
      end
   set mac-acl-default-action assign
end
```

Limiting the number of clients

You might want to prevent overloading of your access point by limiting the number of clients who can associate with it at the same time. Limits can be applied per SSID, per AP, or per radio.

To limit the number of clients per SSID - GUI

1. Go to **WiFI Controller > WiFi Network > SSID** and edit your SSID.
2. Turn on **Maximum Clients** and enter the maximum number of clients in **Limit Concurrent WiFi Clients**.

To limit the number of clients per AP- CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
   edit "FAP221C-default"
      set max-clients 30
   end
```

To limit the number of clients per radio - CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
   edit "FAP221C-default"
      config radio-1
         set max-clients 10
      end
      config radio-2
         set max-clients 30
      end
   end
```

Multicast enhancement

FortiOS can translate multicast traffic into unicast traffic to send to clients, maintaining its own multicast client through IGMP snooping. You can configure this in the CLI:

```
config wireless-controller vap
   edit example_wlan
      set multicast-enhance enable
      set me-disable-thresh 32
   end
```

If the number of clients on the SSID is larger than `me-disable-thresh`, multicast enhancement is disabled.

Dynamic VLAN assignment

You can assign each individual user to a VLAN based on information stored in the RADIUS authentication server. If the user's RADIUS record does not specify a VLAN ID, the user is assigned to the default VLAN for the SSID.

The RADIUS user attributes used for the VLAN ID assignment are:

IETF 64 (Tunnel Type)—Set this to VLAN.

IETF 65 (Tunnel Medium Type)—Set this to 802

IETF 81 (Tunnel Private Group ID)—Set this to the VLAN ID.

To configure dynamic VLAN assignment, you need to:

1. Configure access to the RADIUS server.
2. Create the SSID and enable dynamic VLAN assignment.
3. Create a FortiAP Profile and add the local bridge mode SSID to it.
4. Create the VLAN interfaces and their DHCP servers.
5. Create security policies to allow communication from the VLAN interfaces to the Internet.
6. Authorize the FortiAP unit and assign the FortiAP Profile to it.

To configure access to the RADIUS server

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter a **Name**, the name or IP address in **Primary Server IP/Name**, and the server secret in **Primary Server Secret**.
3. Select **OK**.

To create the dynamic VLAN SSID

1. Go to **WiFi Controller > WiFi Network > SSID**, select Create New and enter:

Name	An identifier, such as dynamic_vlan_ssid.
Traffic Mode	Local bridge or Tunnel, as needed.
SSID	An identifier, such as DYNSSID.
Security Mode	WPA2 Enterprise
Authentication	RADIUS Server. Select the RADIUS server that you configured.

2. Select **OK**.
3. Enable dynamic VLAN in the CLI. Optionally, you can also assign a VLAN ID to set the default VLAN for users without a VLAN assignment.

```
config wireless-controller vap
   edit dynamic_vlan_ssid
      set dynamic-vlan enable
      set vlanid 10
   end
```

To create the FortiAP profile for the dynamic VLAN SSID

1. Go to **WiFi Controller > WiFi Network > FortiAP Profiles**, select Create New and enter:

Name	A name for the profile, such as dyn_vlan_profile.
Platform	The FortiAP model you are using. If you use more than one model of FortiAP, you will need a FortiAP Profile for each model.
Radio 1 and Radio 2	
SSID	Select the SSID you created (example dynamic_vlan_ssid). Do not add other SSIDs.

2. Adjust other radio settings as needed.
3. Select **OK**.

To create the VLAN interfaces

1. Go to **System > Network > Interfaces** and select **Create New**.
2. Enter:

Name	A name for the VLAN interface, such as VLAN100.
Interface	The physical interface associated with the VLAN interface.
VLAN ID	The numeric VLAN ID, for example 100.
Addressing mode	Select Manual and enter the IP address / Network Mask for the virtual interface.
DHCP Server	Enable and then select Create New to create an address range.

3. Select **OK**.
4. Repeat the preceding steps to create other VLANs as needed.

Security policies determine which VLANs can communicate with which other interfaces. These are the simple Firewall Address policy without authentication. Users are assigned to the appropriate VLAN when they authenticate.

To connect and authorize the FortiAP unit

1. Connect the FortiAP unit to the FortiGate unit.
2. Go to **WiFi Controller > Managed Access Points > Managed AP**.

3. When the FortiAP unit is listed, double-click the entry to edit it.
4. In **FortiAP Profile**, select the FortiAP Profile that you created.
5. Select **Authorize**.
6. Select **OK**.

Configuring user authentication

You can perform user authentication when the wireless client joins the wireless network and when the wireless user communicates with another network through a firewall policy. WEP and WPA-Personal security rely on legitimate users knowing the correct key or passphrase for the wireless network. The more users you have, the more likely it is that the key or passphrase will become known to unauthorized people. WPA-Enterprise and captive portal security provide separate credentials for each user. User accounts can be managed through FortiGate user groups or an external RADIUS authentication server.

WPA2 Enterprise authentication

Enterprise authentication can be based on the local FortiGate user database or on a remote RADIUS server. Local authentication is essentially the same for WiFi users as it is for wired users, except that authentication for WiFi users occurs when they associate their device with the AP. Therefore, enterprise authentication must be configured in the SSID. WiFi users can belong to user groups just the same as wired users and security policies will determine which network services they can access.

If your WiFi network uses WPA2 Enterprise authentication verified by a RADIUS server, you need to configure the FortiGate unit to connect to that RADIUS server.

Configuring connection to a RADIUS server - web-based manager

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.
   This name is used in FortiGate configurations. It is not the actual name of the server.
3. In **Primary Server Name/IP**, enter the network name or IP address for the server.
4. In **Primary Server Secret**, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select **OK**.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
   edit exampleRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret aoewmntiasf
   end
```

To implement WPA2 Enterprise security, you select this server in the SSID security settings. See Configuring user authentication on page 830.

To use the RADIUS server for authentication, you can create individual FortiGate user accounts that specify the authentication server instead of a password, and you then add those accounts to a user group. Or, you can add the authentication server to a FortiGate user group, making all accounts on that server members of the user group.

Creating a wireless user group

Most wireless networks require authenticated access. To enable creation of firewall policies specific to WiFi users, you should create at least one WiFi user group. You can add or remove users later. There are two types of user group to consider:

- A Firewall user group can contain user accounts stored on the FortiGate unit or external authentication servers such as RADIUS that contain and verify user credentials.
- A Fortinet Single Sign-On (FSSO) user group is used for integration with Windows Active Directory or Novell eDirectory. The group can contain Windows or Novell user groups who will be permitted access to the wireless LAN.

WiFi Single Sign-On (WSSO) authentication

WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate. For each user, the RADIUS server must provide user group information in the Fortinet-Group-Name attribute. This information is stored in the server's database. After the user authenticates, security policies provide access to network services based on user groups.

1. Configure the RADIUS server to return the Fortinet-Group-Name attribute for each user.
2. Configure the FortiGate to access the RADIUS server, as described in WPA2 Enterprise authentication on page 830.
3. Create firewall user groups on the FortiGate with the same names as the user groups listed in the RADIUS database. Leave the groups empty.
4. In the SSID choose WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you configured.
5. Create security policies as needed, using user groups (**Source User(s)** field) to control access.

When a user authenticates by WSSO, the firewall monitor (**User & Device > Monitor > Firewall**) shows the authentication method as WSSO.

MAC-based authentication

Wireless clients can also be supplementally authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point “vap1” to use RADIUS server hq_radius (configured on the FortiGate):

```
config wireless-controller vap
   edit vap1
      set radius-mac-auth enable
      set radius-mac-auth-server hq_radius
   end
```

Authenticating guest WiFi users

The FortiOS Guest Management feature enables you to easily add guest accounts to your FortiGate unit. These accounts are authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit. To implement guest access, you need to

1. Go to **User & Device > User > User Groups** and create one or more guest user groups.
2. Go to **User & Device > User > Guest Management** to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.

3. Go to **WiFi Controller > WiFi Network > SSID** and configure your WiFi SSID to use captive portal authentication. Select the guest user group(s) that you created.

Guest users can log into the WiFi captive portal with their guest account credentials until the account expires. For more detailed information about creating guest accounts, see “Managing Guest Access” in the Authentication chapter of the FortiOS Handbook.

Configuring firewall policies for the SSID

For users on the WiFi LAN to communicate with other networks, firewall policies are required. This section describes creating a WiFi network to Internet policy.

Before you create firewall policies, you need to define any firewall addresses you will need.

To create a firewall address for WiFi users - web-based manager

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

Name	Enter a name for the address, wifi_net for example.
Type	Select **Subnet.**
Subnet / IP Range	Enter the subnet address, 10.10.110.0/24 for example.
Interface	Select the interface where this address is used, e.g., example_wifi

To create a firewall address for WiFi users - CLI

```
config firewall address
   edit "wifi_net"
      set associated-interface "example_wifi"
      set subnet 10.10.110.0 255.255.255.0
   end
```

To create a firewall policy - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. In **Incoming Interface**, select the wireless interface.
3. In **Source Address**, select the address of your WiFi network, wifi_net for example.
4. In **Outgoing Interface**, select the Internet interface, for example, **port1**.
5. In **Destination Address**, select **All**.
6. In **Service**, select ALL, or select the particular services that you want to allow, and then select the right arrow button to move the service to the **Selected Services** list.
7. In **Schedule**, select **always**, unless you want to define a schedule for limited hours.
8. In **Action**, select ACCEPT.
9. Select **Enable NAT**.
10. Optionally, set up UTM features for wireless users.
11. Select **OK**.

To create a firewall policy - CLI

```
config firewall policy
   edit 0
      set srcintf "example_wifi"
      set dstintf "port1"
      set srcaddr "wifi_net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
   end
```

Configuring the built-in access point on a FortiWiFi unit

Both FortiGate and FortiWiFi units have the WiFi controller feature. If you configure a WiFi network on a FortiWiFi unit, you can also use the built-in wireless capabilities in your WiFi network as one of the access points.

If Virtual Domains are enabled, you must select the VDOM to which the built-in access point belongs. You do this in the CLI. For example:

```
config wireless-controller global
   set local-radio-vdom vdom1
end
```

To configure the FortiWiFi unit's built-in WiFi access point

1. Go to **WiFi Controller > Managed Access Points > Local WiFi Radio**.
2. Make sure that **Enable WiFi Radio** is selected.
3. In **SSID**, if you do not want this AP to carry all SSIDs, select **Select SSIDs** and then select the required SSIDs.
4. Optionally, adjust the **TX Power** slider.
   If you have selected your location correctly (see Configuring the built-in access point on a FortiWiFi unit on page 833), the 100% setting corresponds to the maximum power allowed in your region.
5. If you do not want the built-in WiFi radio to be used for rogue scanning, select **Do not participate in Rogue AP scanning**.
6. Select **OK**.

If you want to connect external APs, such as FortiAP units, see the next chapter, Access point deployment.

Access point deployment

This chapter describes how to configure access points for your wireless network.

Overview
Network topology for managed APs
Discovering and authorizing APs
Advanced WiFi controller discovery
Wireless client load balancing for high-density deployments
LAN port options
Preventing IP fragmentation of packets in CAPWAP tunnels

Overview

FortiAP units discover WiFi controllers. The administrator of the WiFi controller authorizes the FortiAP units that the controller will manage.

In most cases, FortiAP units can find WiFi controllers through the wired Ethernet without any special configuration. Review the following section, Access point deployment on page 834, to make sure that your method of connecting the FortiAP unit to the WiFi controller is valid. Then, you are ready to follow the procedures in Access point deployment on page 834.

If your FortiAP units are unable to find the WiFi controller, refer to Access point deployment on page 834 for detailed information about the FortiAP unit's controller discovery methods and how you can configure them.

Network topology for managed APs

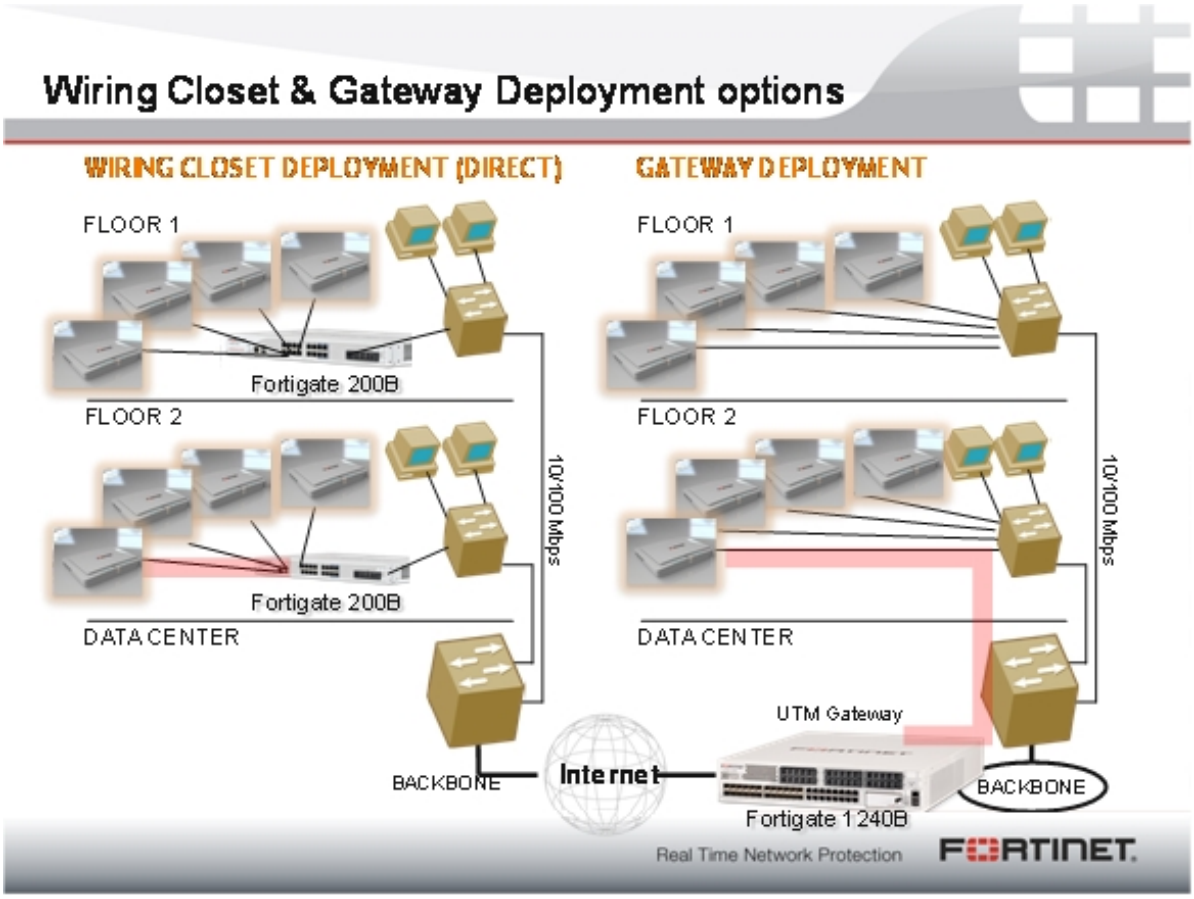
The FortiAP unit can be connected to the FortiGate unit in any of the following ways:

Direct connection: The FortiAP unit is directly connected to the FortiGate unit with no switches between them. This configuration is common for locations where the number of FortiAP's matches up with the number of 'internal' ports available on the FortiGate. In this configuration the FortiAP unit requests an IP address from the FortiGate unit, enters discovery mode and should quickly find the FortiGate WiFi controller. This is also known as a wirecloset deployment. See "Wirecloset and Gateway deployments" below.

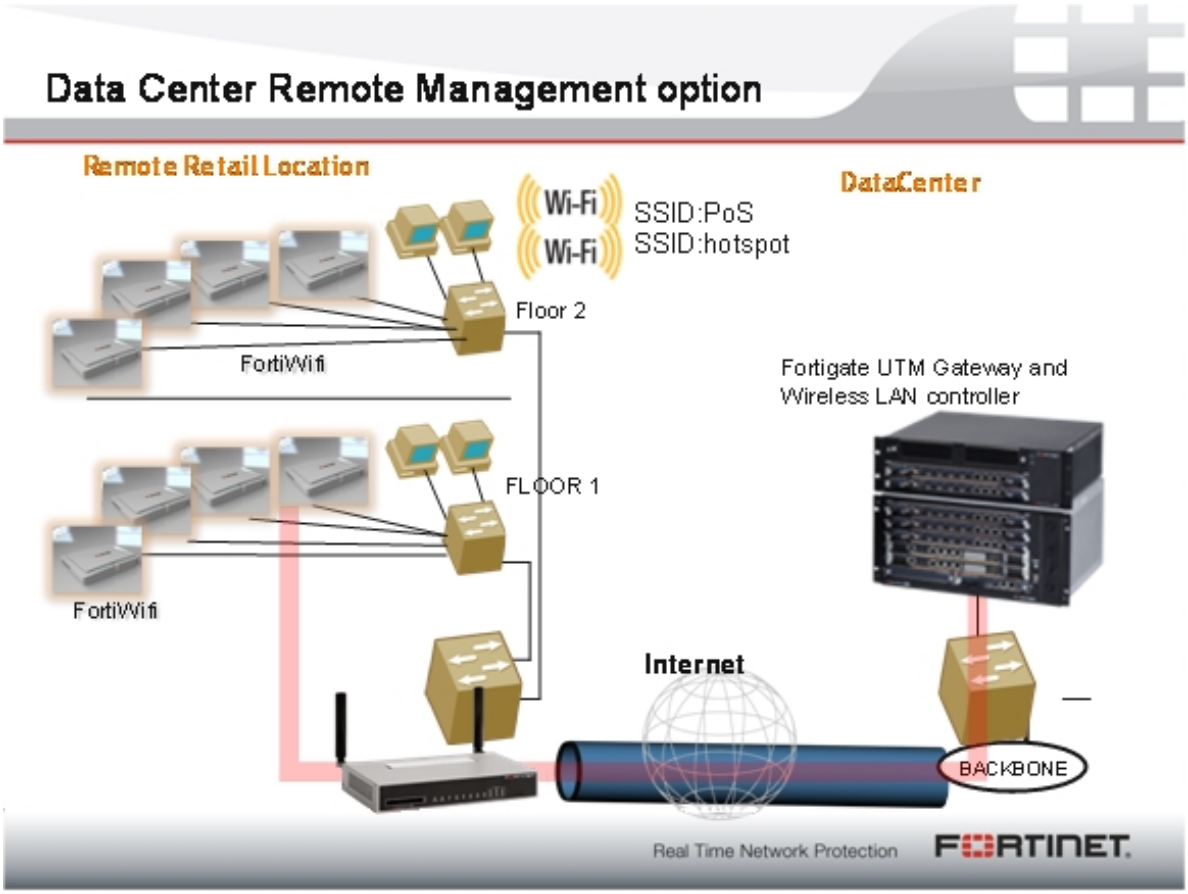
Switched Connection: The FortiAP unit is connected to the FortiGate WiFi controller by an Ethernet switch operating in L2 switching mode or L3 routing mode. There must be a routable path between the FortiAP unit and the FortiGate unit and ports 5246 and 5247 must be open. This is also known as a gateway deployment. See Wirecloset and Gateway deployments below.

Connection over WAN: The FortiGate WiFi controller is off-premises and connected by a VPN tunnel to a local FortiGate. In this method of connectivity its best to configure each FortiAP with the static IP address of the WiFi controller. Each FortiAP can be configured with three WiFi controller IP addresses for redundant failover. This is also known as a datacenter remote management deployment. See Remote deployment below.

Wirecloset and Gateway deployments



Remote deployment



Discovering and authorizing APs

After you prepare your FortiGate unit, you can connect your APs to discover them using the discovery methods described earlier. To prepare the FortiGate unit, you need to

- Configure the network interface to which the AP will connect.
- Configure DHCP service on the interface to which the AP will connect.
- Optionally, preauthorize FortiAP units. They will begin to function when connected.
- Connect the AP units and let the FortiGate unit discover them.
- Enable each discovered AP and configure it or assign it to an AP profile.

Configuring the network interface for the AP unit

The interface to which you connect your wireless access point needs an IP address. No administrative access, DNS Query service or authentication should be enabled.

To configure the interface for the AP unit - web-based manager

1. Go to **System > Network > Interfaces** and edit the interface to which the AP unit connects.
2. Set **Addressing Mode** to **Dedicate to Extension Device.**
3. Enter the IP address and netmask to use.
   This FortiGate unit automatically configures a DHCP server on the interface that will assign the remaining higher addresses up to .254 to FortiAP units. For example, if the IP address is 10.10.1.100, the FortiAP units will be assigned 10.10.1.101 to 10.10.1.254. To maximize the available addresses, use the .1 address for the interface: 10.10.1.1, for example.
4. Select **OK**.

To configure the interface for the AP unit - CLI

In the CLI, you must configure the interface IP address and DHCP server separately.

```
config system interface
   edit port3
      set mode static
      set ip 10.10.70.1 255.255.255.0
   end
config system dhcp server
   edit 0
      set interface "dmz"
      config ip-range
         edit 1
            set end-ip 10.10.70.254
            set start-ip 10.10.70.2
         end
      set netmask 255.255.255.0
      set vci-match enable
      set vci-string "FortiAP"
   end
```

The optional `vci-match` and `vci-string` fields ensure that the DHCP server will provide IP addresses only to FortiAP units.

Pre-authorizing a FortiAP unit

If you enter the FortiAP unit information in advance, it is authorized and will begin to function when it is connected.

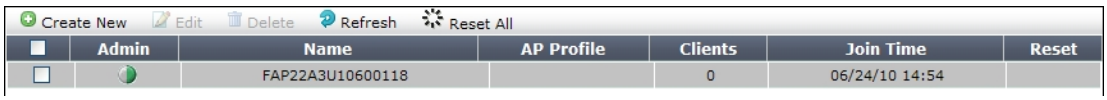
To pre-authorize a FortiAP unit

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and select **Create New**.
   On some models the **WiFi Controller** menu is called **WiFi & Switch Controller**.
2. Enter the **Serial Number** of the FortiAP unit.
3. Configure the **Wireless Settings** as required.
4. Select **OK**.

Enabling and configuring a discovered AP

Within two minutes of connecting the AP unit to the FortiGate unit, the discovered unit should be listed on **WiFi Controller > Managed Access Points > Managed FortiAP** page.

Discovered access point unit



When you authorize (enable) a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). You can create and select a different profile if needed. The FortiAP Profile defines the entire configuration for the AP.

To add and configure the discovered AP unit - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAP**.
   This configuration also applies to local WiFi radio on FortiWiFi models.
2. Select the FortiAP unit from the list and edit it.
3. Optionally, enter a **Name**. Otherwise, the unit will be identified by serial number.
4. Select **Authorize**.
5. Select a **FortiAP Profile**.
6. If you want to override the FortiAP profile, select **Override Settings** and adjust the following:

Enable WiFi Radio	This must be selected to enable operation of this AP.
SSID	**Automatically Inherit all SSIDs** — AP will carry all WiFi networks. **Select SSIDs** — select individual SSIDs for this AP to carry.
Auto TX Power Control	If you enable automatic transmitter power control, adjust TX Power Low and TX Power High to set the power range.
Tx Power	If you are not using automatic power control, adjust AP transmitter power. The 100% setting is the maximum permitted in your country. See Configuring a WiFi LAN on page 815.
Do not participate in Rogue AP scanning	Select this option if scanning adversely affects WiFi traffic.

7. Select **OK**.

The physical access point is now added to the system. If the rest of the configuration is complete, it should be possible to connect to the wireless network through the AP.

To add the discovered AP unit - CLI

First get a list of the discovered access point unit serial numbers:

```
get wireless-controller wtp
```

Add a discovered unit and associate it with AP-profile1, for example:

```
config wireless-controller wtp
  edit FAP22A3U10600118
    set admin enable
    set wtp-profile AP-profile1
  end
```

To use the default profile, leave the `wtp-profile` field unset.

To view the status of the added AP unit

```
config wireless-controller wtp
  edit FAP22A3U10600118
  get
```

The `join-time` field should show a time, not “N/A”. See the preceding web-based manager procedure for more information.

Assigning the same profile to multiple FortiAP units

The same profile can now be applied to multiple managed FortiAP units at the same time. To do this, do the following:

1. Go to **WiFi Controller** > **Managed Access Points** > **Managed FortiAPs** to view the AP list.
2. Select all FortiAP units you wish to apply the profile to.
3. Right click on one of the selected FortiAPs and select **Assign Profile**.
4. Choose the profile you wish to apply.

Connecting to the FortiAP CLI

The FortiAP unit has a CLI through which some configuration options can be set. You can access the CLI using Telnet.

To access the FortiAP unit CLI through the FortiAP Ethernet port

1. Connect your computer to the FortiAP Ethernet interface, either directly with a cross-over cable or through a separate switch or hub.
2. Change your computer’s IP address to 192.168.1.3
3. Telnet to IP address 192.168.1.2.
   Ensure that FortiAP is in a private network with no DHCP server for the static IP address to be accessible.
4. Login with user name admin and no password.
5. Enter commands as needed.
6. Optionally, use the `passwd` command to assign an administrative password for better security.
7. Save the configuration by entering the following command:
   ```
   cfg -c .
   ```
8. Unplug the FortiAP and then plug it back in, in order for the configuration to take effect

To access the FortiAP unit CLI through the FortiGate unit

1. Connect the FortiAP unit to the FortiGate network interface that has been configured for FortiAP units.
2. Use the FortiGate CLI `execute telnet` command to access the FortiAP. For example, if the FortiAP unit IP address is 192.168.1.2, enter:
   ```
   execute telnet 192.168.1.2
   ```
3. At the FortiAP login prompt, enter `admin`. When you are finished using the FortiAP CLI, enter `exit`.

When a WiFi controller has taken control of the FortiAP unit, Telnet access to the FortiAP unit’s CLI is no longer available.

Checking and updating FortiAP unit firmware

You can view and update the FortiAP unit's firmware from the FortiGate unit that acts as its WiFi controller.

Checking the FortiAP unit firmware version

Go to **WiFi Controller > Managed Access Points > Managed FortiAP** to view the list of FortiAP units that the FortiGate unit can manage. The **OS Version** column shows the current firmware version running on each AP.

Updating FortiAP firmware from the FortiGate unit

You can update the FortiAP firmware using either the web-based manager or the CLI. Only the CLI method can update all FortiAP units at once.

To update FortiAP unit firmware - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAP**.
2. Select the FortiAP unit from the list and edit it.
3. In **FortiAP OS Version**, select **Upgrade from File**.
4. Select **Browse** and locate the firmware upgrade file.
5. Select **OK**.
6. When the upgrade process completes, select **OK**.
   The FortiAP unit restarts.

To update FortiAP unit firmware - CLI

1. Upload the FortiAP image to the FortiGate unit.
   For example, the Firmware file is FAP_22A_v4.3.0_b0212_fortinet.out and the server IP address is 192.168.0.100.
   ```
   execute wireless-controller upload-wtp-image tftp FAP_22A_v4.3.0_b0212_fortinet.out
       192.168.0.100
   ```
   If your server is FTP, change `tftp` to `ftp`, and if necessary add your user name and password at the end of the command.
2. Verify that the image is uploaded:
   ```
   execute wireless-controller list-wtp-image
   ```
3. Upgrade the FortiAP units:
   ```
   exec wireless-controller reset-wtp all
   ```
   If you want to upgrade only one FortiAP unit, enter its serial number instead of `all`.

Updating FortiAP firmware from the FortiAP unit

You can connect to a FortiAP unit's internal CLI to update its firmware from a TFTP server on the same network. This method does not require access to the wireless controller.

1. Place the FortiAP firmware image on a TFTP server on your computer.
2. Connect the FortiAP unit to a separate private switch or hub or directly connect to your computer via a cross-over cable.
3. Change your computer's IP address to 192.168.1.3.

4. Telnet to IP address 192.168.1.2.
   This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.
5. Login with the username “admin” and no password.
6. Enter the following command.
   For example, the FortiAP image file name is FAP_22A_v4.3.0_b0212_fortinet.out.

```
restore FAP_22A_v4.3.0_b0212_fortinet.out 192.168.1.3
```

Advanced WiFi controller discovery

A FortiAP unit can use any of four methods to locate a controller. By default, FortiAP units cycle through all four of the discovery methods. In most cases there is no need to make configuration changes on the FortiAP unit.

There are exceptions. The following section describes the WiFi controller discovery methods in more detail and provides information about configuration changes you might need to make so that discovery will work.

Controller discovery methods

There are four methods that a FortiAP unit can use to discover a WiFi controller.

Static IP configuration

If FortiAP and the controller are not in the same subnet, broadcast and multicast packets cannot reach the controller. The admin can specify the controller’s static IP on the AP unit. The AP unit sends a discovery request message in unicast to the controller. Routing must be properly configured in both directions.

To specify the controller’s IP address on a FortiAP unit

```
cfg -a AC_IPADDR_1="192.168.0.100"
```

By default, the FortiAP unit receives its IP address, netmask, and gateway address by DHCP. If you prefer, you can assign these statically.

To assign a static IP address to the FortiAP unit

```
cfg -a ADDR_MODE=STATIC
cfg -a AP_IPADDR="192.168.0.100"
cfg -a AP_NETMASK="255.255.255.0"
cfg -a IPGW=192.168.0.1
cfg -c
```

For information about connecting to the FortiAP CLI, see Advanced WiFi controller discovery on page 841.

Broadcast request

The AP unit broadcasts a discovery request message to the network and the controller replies. The AP and the controller must be in the same broadcast domain. No configuration adjustments are required.

Multicast request

The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message. The AP and the controller do not need to be in the same broadcast domain if multicast routing is properly configured.

The default multicast destination address is 224.0.1.140. It can be changed through the CLI. The address must be same on the controller and AP.

To change the multicast address on the controller

```
config wireless-controller global
   set discovery-mc-addr 224.0.1.250
end
```

To change the multicast address on a FortiAP unit

```
cfg -a AC_DISCOVERY_MC_ADDR="224.0.1.250"
```

For information about connecting to the FortiAP CLI, see Advanced WiFi controller discovery on page 841.

DHCP

If you use DHCP to assign an IP address to your FortiAP unit, you can also provide the WiFi controller IP address at the same time. This is useful if the AP is located remotely from the WiFi controller and other discovery techniques will not work.

When you configure the DHCP server, configure Option 138 to specify the WiFi controller IP address. You need to convert the address into hexadecimal. Convert each octet value separately from left to right and concatenate them. For example, 192.168.0.1 converts to C0A80001.

If Option 138 is used for some other purpose on your network, you can use a different option number if you configure the AP units to match.

To change the FortiAP DHCP option code

To use option code 139 for example, enter

```
cfg -a AC_DISCOVERY_DHCP_OPTION_CODE=139
```

For information about connecting to the FortiAP CLI, see Advanced WiFi controller discovery on page 841.

Wireless client load balancing for high-density deployments

Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- Access Point Hand-off - the wireless controller signals a client to switch to another access point.
- Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Load balancing is not applied to roaming clients.

Access point hand-off

Access point handoff wireless load balancing involves the following:

- If the load on an access point (ap1) exceeds a threshold (of for example, 30 clients) then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2).

- When one or more access points are overloaded (for example, more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy access point that is closest to the new client and this access point is the one that responds to the client and the one that the client joins.

Frequency hand-off or band-steering

Encouraging clients to use the 5GHz WiFi band if possible enables those clients to benefit from faster interference-free 5GHz communication. The remaining 2.4GHz clients benefit from reduced interference.

The WiFi controller probes clients to determine their WiFi band capability. It also records the RSSI (signal strength) for each client on each band.

If a new client attempts to join the network, the controller looks up that client's MAC address in its wireless device table and determines if it's a dual band device. If it is not a dual band device, then its allowed to join. If it is a dual band device, then its RSSI on 5GHz is used to determine whether the device is close enough to an access point to benefit from movement to 5GHz frequency.

If both conditions of 1) dual band device and 2) RSSI value is strong, then the wireless controller does not reply to the join request of the client. This forces the client to retry a few more times and then timeout and attempt to join the same SSID on 5GHz. Once the Controller see this new request on 5GHz, the RSSI is again measured and the client is allowed to join. If the RSSI is below threshold, then the device table is updated and the controller forces the client to timeout again. A client's second attempt to connect on 2.4GHz will be accepted.

Configuration

From the web-based manager, edit a custom AP profile and select **Frequency Handoff** and **AP Handoff** as required for each radio on the AP.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile. Enable access point hand-off and frequency hand-off separately for each radio in the custom AP profile.

```
config wireless-controller wtp-profile
   edit new-ap-profile
      set handoff-rssi <rssi_int>
      set handoff-sta-thresh <clients_int>
      config radio-1
         set frequency-handoff {disable | enable}
         set ap-handoff {disable | enable}
      end
      config radio-2
         set frequency-handoff {disable | enable}
         set ap-handoff {disable | enable}
      end
   end
```

Where:

- `handoff-rssi` is the RSSI threshold. Clients with a 5 GHz RSSI threshold over this value are load balanced to the 5GHz frequency band. Default is 25. Range is 20 to 30.
- `handoff-sta-thresh` is the access point handoff threshold. If the access point has more clients than this threshold it is considered busy and clients are changed to another access point. Default is 30, range is 5 to 25.
- `frequency-handoff` enable or disable frequency handoff load balancing for this radio. Disabled by default.
- `ap-handoff` enable or disable access point handoff load balancing for this radio. Disabled by default.

Frequency handoff must be enabled on the 5GHz radio to learn client capability.

LAN port options

Some FortiAP models have one or more ethernet interfaces marked LAN. These ports can provide wired network access. LAN ports are bridged to either the wired WAN interface or to one of the WiFi SSIDs that the FortiAP unit carries.

Bridging a LAN port with an SSID

Bridging a LAN port with a FortiAP SSID combines traffic from both sources to provide a single broadcast domain for wired and wireless users.

In this configuration

- The IP addresses for LAN clients come from the DHCP server that serves the wireless clients.
- Traffic from LAN clients is bridged to the SSID's VLAN. Dynamic VLAN assignment for hosts on the LAN port is not supported.
- Wireless and LAN clients are on the same network and can communicate locally, via the FortiAP.
- Any host connected to the LAN port will be taken as authenticated. RADIUS MAC authentication for hosts on the LAN port is not supported.

For configuration instructions, see LAN port options on page 844.

Bridging a LAN port with the WAN port

Bridging a LAN port with the WAN port enables the FortiAP unit to be used as a hub which is also an access point.

In this configuration

- The IP addresses for LAN clients come from the WAN directly and will typically be in the same range as the AP itself.
- All LAN client traffic is bridged directly to the WAN interface.
- Communication between wireless and LAN clients can only occur if a policy on the FortiGate unit allows it.

For configuration instructions, see LAN port options on page 844.

Configuring FortiAP LAN ports

You can configure FortiAP LAN ports for APs in a FortiAP Profile. A profile applies to APs that are the same model and share the same configuration. If you have multiple models or different configurations, you might need to create several FortiAP Profiles. For an individual AP, it is also possible to override the profile settings.

To configure FortiAP LAN ports in a FortiAP Profile - web-based manager

1. Go to **WiFi Controller > FortiAP Profiles.**
2. Edit the default profile for your FortiAP model or select **Create New**.
3. If you are creating a new profile, enter a **Name** and select the correct **Platform** (model).
4. Select SSIDs.
5. In the **LAN Port** section, set **Mode** to **Bridge to** and select an SSID or **WAN Port** as needed.
   On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually. Enable each port that you want to use and select an SSID or **WAN Port** as needed.
6. Select **OK**.

Be sure to select this profile when you authorize your FortiAP units.

To configure FortiAP LAN ports - CLI

In this example, the default FortiAP-11C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
   edit FAP11C-default
      config lan
         set port-mode bridge-to-ssid
         set port-ssid office
      end
   end
end
```

In this example, the default FortiAP-28C profile is configured to bridge LAN port1 to the office SSID and to bridge the other LAN ports to the WAN port.

```
config wireless-controller wtp-profile
   edit FAP28C-default
      config lan
         set port1-mode bridge-to-ssid
         set port1-ssid office
         set port2-mode bridge-to-wan
         set port3-mode bridge-to-wan
         set port4-mode bridge-to-wan
         set port5-mode bridge-to-wan
         set port6-mode bridge-to-wan
         set port7-mode bridge-to-wan
         set port8-mode bridge-to-wan
      end
   end
```

To configure FortiAP unit LAN ports as a FortiAP Profile override - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.
   On FortiGate models 100D, 600C, 800C, and 1000C, go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**.
2. Select the FortiAP unit from the list and select **Edit**.
3. Select the **FortiAP Profile**, if this has not already been done.
4. Enable **Override Settings**.
5. In the **LAN Port** section, set **Mode** to **Bridge to** and select an SSID or **WAN Port** as needed.
   On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually. Enable each port that you want to use and select an SSID or **WAN Port** as needed.
6. Select **OK**.

To configure FortiAP unit LAN ports as a FortiAP Profile override - CLI

In this example, a FortiAP unit's configuration overrides the FortiAP Profile to bridge the LAN port to the WAN port.

```
config wireless-controller wtp
   edit FAP11C3X13000412
      set wtp-profile FAP11C-default
      set override-profile enable
      config lan
         set port-mode bridge-to-wan
      end
```

```
    end
```

Preventing IP fragmentation of packets in CAPWAP tunnels

A common problem with controller-based WiFi networks is reduced performance due to IP fragmentation of the packets in the CAPWAP tunnel.

Fragmentation can occur because of CAPWAP tunnel overhead increasing packet size. If the original wireless client packets are close to the maximum transmission unit (MTU) size for the network (usually 1500 bytes for Ethernet networks unless jumbo frames are used) the resulting CAPWAP packets may be larger than the MTU, causing the packets to be fragmented. Fragmenting packets can result in data loss, jitter, and decreased throughput.

The FortiOS/FortiAP solution to this problem is to cause wireless clients to send smaller packets to FortiAP devices, resulting in 1500-byte CAPWAP packets and no fragmentation. The following options configure CAPWAP IP fragmentation control:

```
config wireless-controller wtp-profile
   edit new-wtp
      set ip-fragment-preventing tcp-mss-adjust icmp-unreachable
      set tun-mtu-uplink {0 | 576 | 1500}
      set tun-mtu-downlink {0 | 576 | 1500}
   end
end
```

By default, `tcp-mss-adjust` and `icmp-unreachable` are not enabled, and `tun-mtu-uplink` and `tun-mtu-downlink` are set to 0.

To set `tun-mtu-uplink` and `tun-mtu-downlink`, use the default TCP MTU value of 1500. This default configuration prevents packet fragmentation because the FortiAP unit limits the size of TCP packets received from wireless clients so the packets don't have to be fragmented before CAPWAP encapsulation.

The `tcp-mss-adjust` option causes the FortiAP unit to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. The FortiAP does this by adding a reduced MSS value to the SYN packets sent by the FortiAP unit when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the `tun-mtu-uplink` setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the `tun-mtu-uplink` size.

The `icmp-unreachable` option affects all traffic (UDP and TCP) between wireless clients and the FortiAP unit. This option causes the FortiAP unit to drop packets that have the "Don't Fragment" bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet -- type 3 "ICMP Destination unreachable" with code 4 "Fragmentation Needed and Don't Fragment was Set" back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

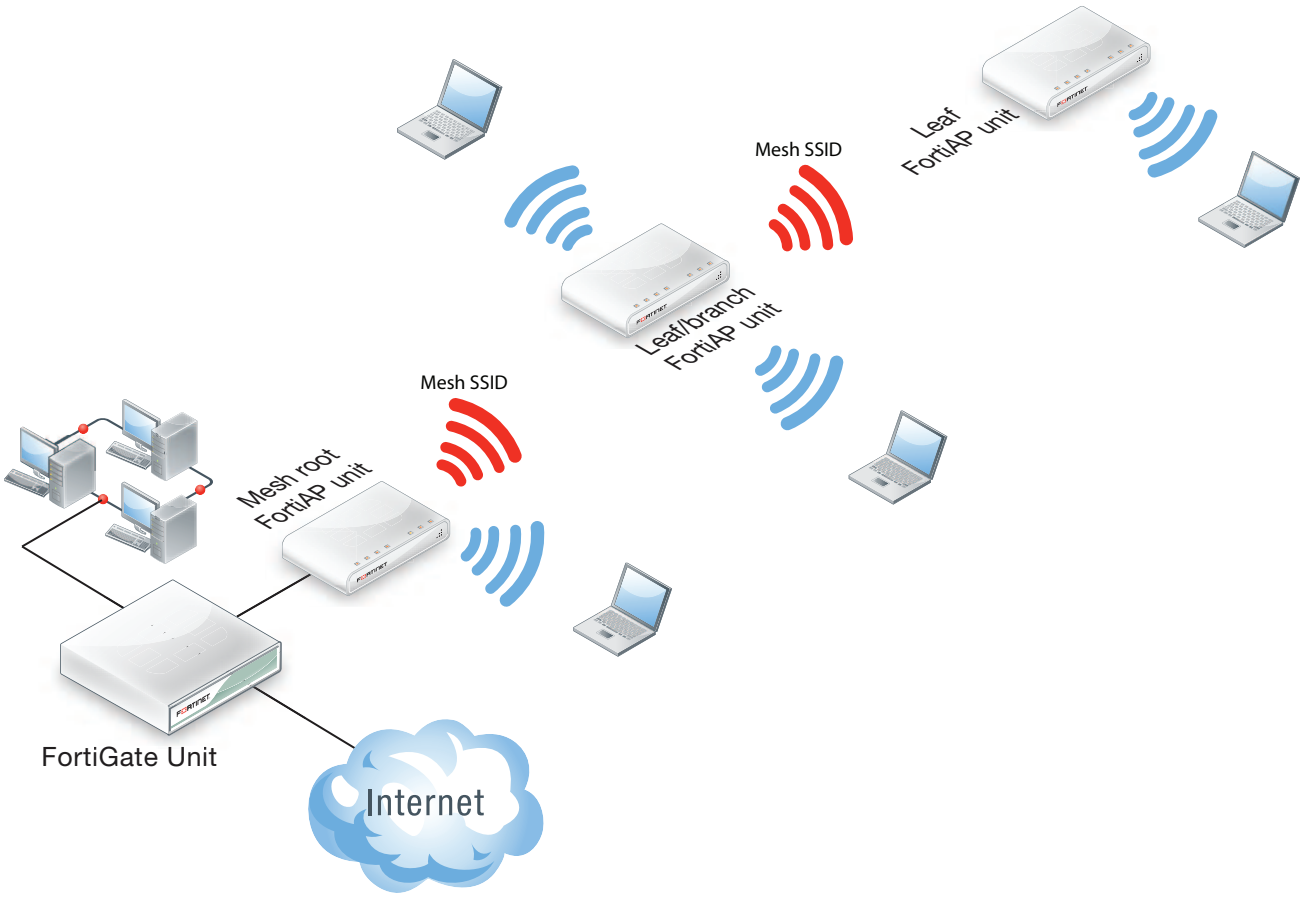
Wireless Mesh

The access points of a WiFi network are usually connected to the WiFi controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

Overview of Wireless Mesh
Configuring a meshed WiFi network
Configuring a point-to-point bridge

Overview of Wireless Mesh

The figure below shows a wireless mesh topology.



The AP that is connected to the network by Ethernet is called the Mesh Root node. It is configured with an SSID (also called a virtual access point or VAP) dedicated to backhaul communication with the remote FortiAP units. The backhaul SSID carries CAPWAP discovery, configuration, and other communications that would usually be carried on an Ethernet connection. Regular WiFi clients cannot connect to the backhaul SSID. They connect to the regular SSIDs carried on the access points.

The root node can be a FortiAP unit or the built-in AP of a FortiWiFi unit. APs that serve only regular WiFi clients are called Leaf nodes. Leaf APs that also carry the mesh SSID for more distant Leaf nodes are called Leaf/branch nodes.

All access points in a wireless mesh configuration must have at least one of their radios configured to provide mesh backhaul communication. As with wired APs, when mesh APs start up they can be discovered by a FortiGate or FortiWiFi unit WiFi controller and authorized to join the network.

The backhaul SSID delivers the best performance when it is carried on a dedicated radio. On a two-radio FortiAP unit, for example, the 5GHz radio could carry only the backhaul SSID while the 2.4GHz radio carries one or more SSIDs that serve users. Background WiFi scanning is possible in this mode.

The backhaul SSID can also share the same radio with SSIDs that serve users. Performance is reduced because the backhaul and user traffic compete for the available bandwidth. Background WiFi scanning is not available in this mode. One advantage of this mode is that a two-radio AP can offer WiFi coverage on both bands.

The root mesh AP is the AP unit that has a wired Ethernet connection to the WiFi controller. The AP units that are wirelessly linked to the controller over the backhaul SSID are called branch or leaf APs.

Wireless mesh deployment modes

There are two common wireless mesh deployment modes:

Wireless Mesh	Access points are wirelessly connected to a FortiGate or FortiWiFi unit WiFi controller. WiFi users connect to wireless SSIDs in the same way as on non-mesh WiFi networks.
Wireless bridging	Two LAN segments are connected together over a wireless link (the backhaul SSID). On the leaf AP, the Ethernet connection can be used to provide a wired network. Both WiFi and wired users on the leaf AP are connected to the LAN segment to which the root AP is connected.

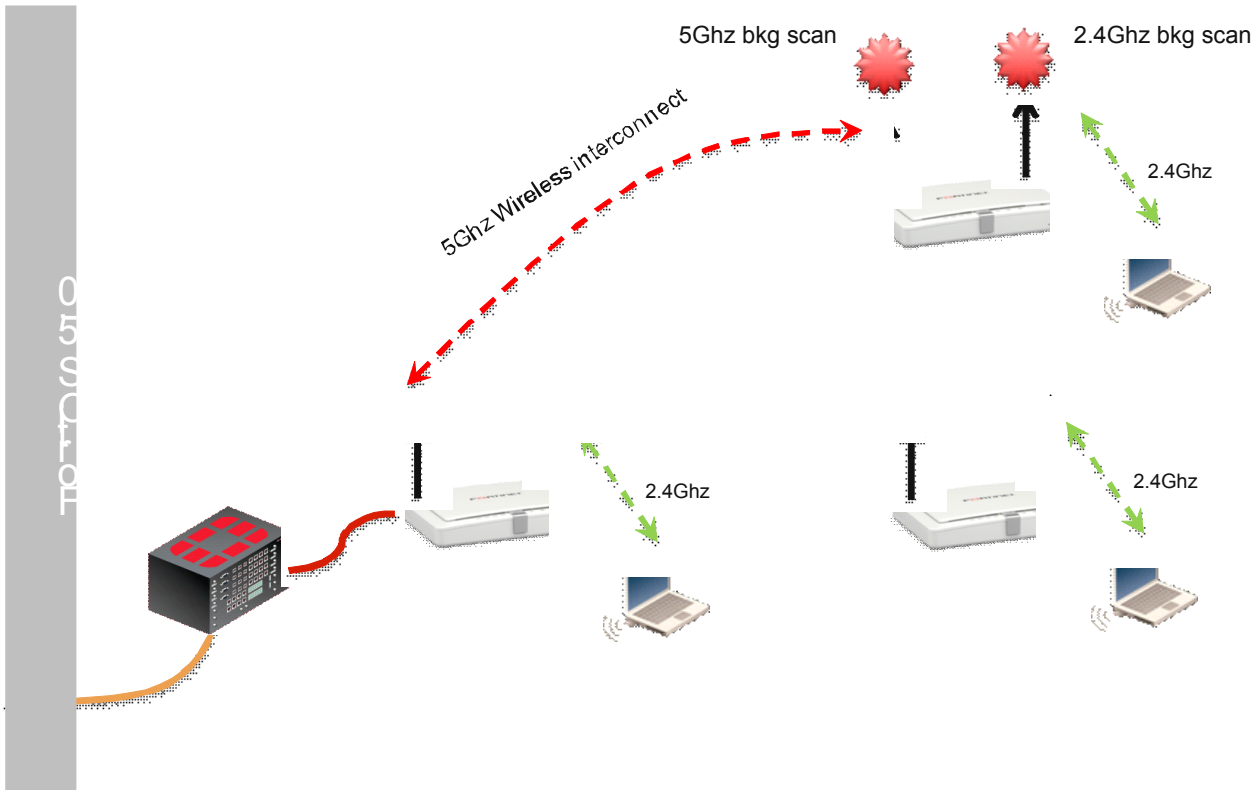
Firmware requirements

All FortiAP units that will be part of the wireless mesh network must be upgraded to FAP firmware version 5.0 build 003. FortiAP-222B units must have their BIOS upgraded to version 400012. The FortiWiFi or FortiGate unit used as the WiFi controller must be running FortiOS 5.0.

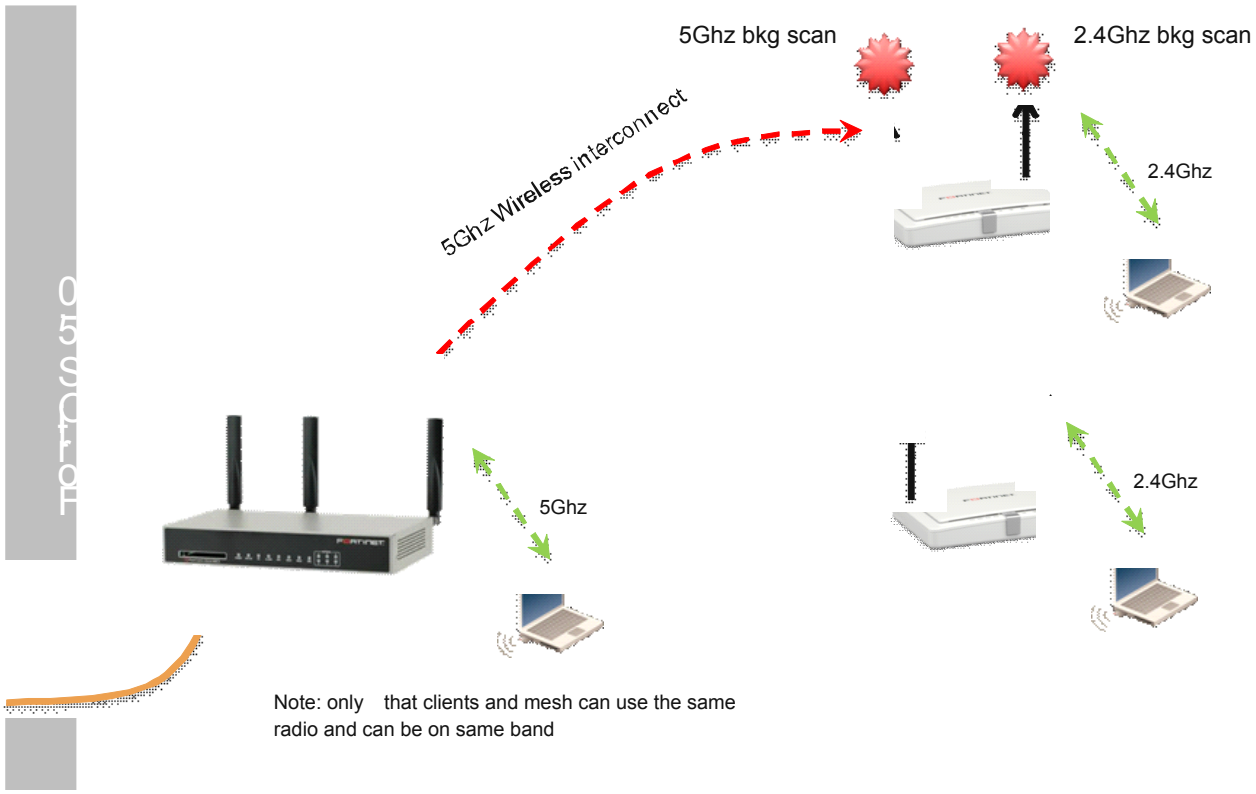
Types of wireless mesh

A WiFi mesh can provide access to widely-distributed clients. The root mesh AP which is directly connected to the WiFi controller can be either a FortiAP unit or the built-in AP of a FortiWiFi unit that is also the WiFi controller.

FortiAP units used as both mesh root AP and leaf AP

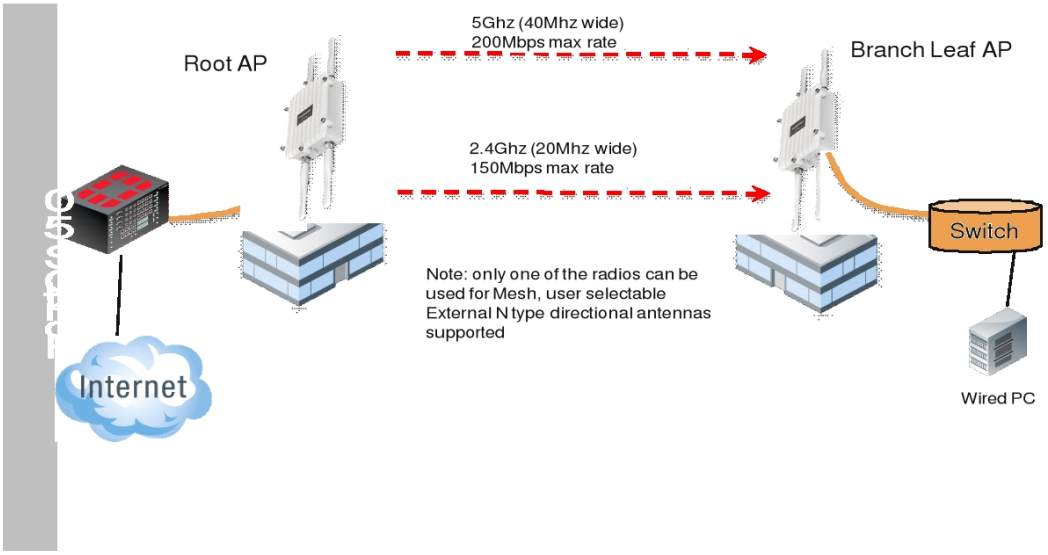


FortiWiFi unit as root mesh AP with FortiAP units as leaf APs



An alternate use of the wireless mesh functionality is as a point-to-point relay. Both wired and WiFi users on the leaf AP side are connected to the LAN segment on the root mesh side.

Point-to-point wireless mesh



Configuring a meshed WiFi network

Each VDOM on the FortiGate unit contains a predefined WiFi mesh interface named wl.mesh and a predefined SSID (which cannot be deleted) named fortinet.mesh.<vdom-name>. You can create additional mesh SSIDs. Create the SSID with **Traffic Mode** set to **Mesh Downlink**.

You need to:

- Create custom AP profiles, if you are not using the automatic AP profile.
- Configure the mesh root AP, either a FortiWiFi unit's Local Radio or a FortiAP unit.
- Configure mesh branch/leaf AP units.
- Authorize the mesh branch/leaf units when they connect to the WiFi Controller.

Creating custom AP profiles

You can apply the automatic AP profile or create one or more custom AP profiles for the mesh root and branch/leaf APs. A custom profile provides more control over which radio channels are used, intrustion protection, load balancing, background rogue AP scanning, and so on. Typically, the custom profiles are configured so that Radio 1 (5GHz) carries the mesh backhaul SSID while Radio 2 (2.4GHz) carries the SSIDs to which users connect.

For more information, see Configuring a WiFi LAN on page 815.

Configuring the mesh root AP

The mesh root AP can be either a FortiWiFi unit's built-in AP or a FortiAP unit.

To enable a FortiWiFi unit's Local Radio as mesh root - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Local WiFi Radio**.
2. Select **Enable WiFi Radio**.
3. In **SSID**, select **Select SSIDs**, then select **fortinet.mesh.root**.
4. Optionally, adjust **TX Power** or select **Auto Tx Power Control**.
5. Select **Apply**.

In a network with multiple wireless controllers, you need to change the mesh SSID so that each mesh root has a unique SSID. Other controllers using the same mesh root SSID might be detected as fake or rogue APs. Go to **WiFi Controller > WiFI Network > SSID** to change the SSID.

Fortinet also recommends that you create a new preshared key instead of using the default.

To configure a network interface for the FortiAP unit

1. On the FortiGate unit, go to **System > Network > Interfaces**.
2. Select the interface where you will connect the FortiAP unit and edit it.
3. In **Addressing mode**, select **Manual**.

4. In **IP/Network Mask**, enter an IP address and netmask for the interface.
   To maximize the number of addresses available for clients, the interface address should end with 1, for example 192.168.10.1.
5. In **DHCP Server** select **Enable**.
   An **Address Range** is entered automatically. It consists of the subnet address space above the interface address. For example, if the interface IP/mask is 192.168.10.100/24, the DHCP address range is 192.168.10.101 through 192.168.10.254.
6. Select **OK**.

To enable a FortiAP unit as mesh root - web-based manager

1. Connect the root FortiAP unit's Ethernet port to the FortiGate network interface that you configured for it. Connect the FortiAP unit to its power source.
2. Go to **WiFi Controller > Managed Access Points > Managed FortiAP**.
   If the root FortiAP unit is not listed, wait 15 seconds and select **Refresh**. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the root FortiAP unit and try again.
3. Select the discovered FortiAP unit and edit its settings.
4. Select the **FortiAP Profile** to apply.
5. In **State**, select **Authorize**.
6. Select **OK**.

You need to create firewall policies to permit traffic to flow from the network interface where the FortiAP unit is connected to the network interfaces for the Internet and other networks. Enable NAT.

Configuring the mesh branches or leaves

The FortiAP units that will serve as branch/leaf nodes must be preconfigured.

1. Connect to the FortiAP unit web-based manager on its default Ethernet interface IP address, 192.168.1.2.
2. In the **Connectivity** section enter:

Uplink	Mesh
Mesh AP SSID	fortinet.mesh.<vdom-name> For example, for the root domain, fortinet.mesh.root.
Mesh AP Password	Same as Mesh AP SSID.
Ethernet Bridge	Select

3. Select **Apply** and then select **Logout**.

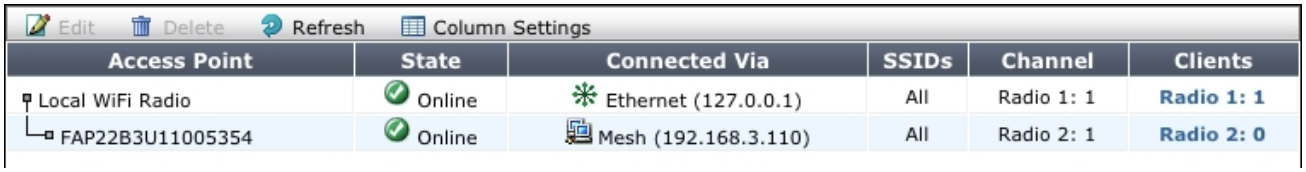
Authorizing mesh branch/leaf APs

The pre-configured branch/leaf FortiAP units will connect themselves wirelessly to the WiFi Controller through the mesh network. You must authorize each unit

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAP**. Periodically select **Refresh** until the FortiAP unit is listed.
   The **State** of the FortiAP unit should be **Waiting for Authorization**.
2. Open the FortiAP entry for editing.
3. Select the **FortiAP Profile** to apply.

4. Select **Authorize**.
5. Select **OK**.
   Initially, the **State** of the FortiAP unit is **Offline**. Periodically select **Refresh** to update the status. Within about two minutes, the state changes to **Online**.

FortiWiFi unit as root mesh with FortiAP unit as branch/leaf node



Viewing the status of the mesh network

Go to **WiFi Controller > Managed Access Points > Managed FortiAP** to view the list of APs. The **Connected Via** field shows **Mesh** for mesh-connected units and lists the IP address to which they connect.

In the FortiAP CLI, you can check the `main ip` field in the output from the command

```
cw_diag -c mesh
```

Configuring a point-to-point bridge

You can create a point-to-point bridge to connect two wired network segments using a WiFi link. The effect is the same as connecting the two network segments to the same wired switch.

You need to:

- Configure a backhaul link and root mesh AP as described in Configuring a point-to-point bridge on page 853.
  Note: The root mesh AP for a point-to-point bridge must be a FortiAP unit, not the internal AP of a FortiWiFi unit.
- Configure bridging on the leaf AP unit.

To configure the leaf AP unit for bridged operation - FortiAP web-based manager

1. With your browser, connect to the FortiAP unit web-based manager.
   You can temporarily connect to the unit's Ethernet port and use its default address: 192.168.1.2.
2. Enter:

Operation Mode	Mesh
Mesh AP SSID	fortinet-ap
Mesh AP Password	fortinet
Ethernet Bridge	Select

3. Select **Apply**.
4. Connect the local wired network to the Ethernet port on the FortiAP unit.
   Users are assigned IP addresses from the DHCP server on the wired network connected to the root mesh AP unit.

To configure a FortiAP unit as a leaf AP - FortiAP CLI

```
cfg -a MESH_AP_SSID=fortinet-ap
cfg -a MESH_AP_PASSWD=fortinet
cfg -a MESH_ETH_BRIDGE=1
cfg -a MESH_AP_TYPE=1
cfg -c
```

Combining WiFi and wired networks with a software switch

Combining WiFi and wired networks with a software switch
FortiAP local bridging (Private Cloud-Managed AP)
Using bridged FortiAPs to increase scalability

Combining WiFi and wired networks with a software switch

A WiFi network can be combined with a wired LAN so that WiFi and wired clients are on the same subnet. This is a convenient configuration for users. Note that software switches are only available if your FortiGate is in Interface mode.

Wireless Mesh features cannot be used in conjunction with this configuration because they enable the FortiAP Local Bridge option.

To create the WiFi and wired LAN configuration, you need to:

- Configure the SSID so that traffic is tunneled to the WiFi controller.
- Configure a software switch interface on the FortiGate unit with the WiFi and internal network interface as members.
- Configure Captive Portal security for the software switch interface.

To configure the SSID - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Enter:

Interface name	A name for the new WiFi interface, `homenet_if` for example.
Traffic Mode	Tunnel to Wireless Controller
SSID	The SSID visible to users, `homenet` for example.
Security Mode **Data Encryption** **Preshared Key**	Configure security as you would for a regular WiFi network.

3. Select **OK**.
4. Go to **WiFi Controller > Managed Access Points > Managed FortiAP,** select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
   The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

To configure the SSID - CLI

This example creates a WiFi interface “homenet_if” with SSID “homenet” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
```

```
    edit "homenet_if"
      set vdom "root"
      set ssid "homenet"
      set security wpa-personal
      set passphrase "Fortinet1"
    end
  config wireless-controller wtp
    edit FAP22B3U11005354
      set admin enable
      set vaps "homenet_if"
    end
```

To configure the FortiGate unit - web-based manager

1. Go to **System > Network > Interfaces** and select **Create New**.
2. Enter:

Interface Name	A name for the new interface, `homenet_nw` for example.
Type	Software Switch
Interface Members	Add homenet_if and the internal network interface.
Addressing Mode	Select Manual and enter an address, for example `172.16.96.32/255.255.255.0`
DHCP Server	Enable and configure an address range for clients.
Security Mode	Select **Captive Portal**. Add the permitted **User Groups**.

3. Select **OK**.

To configure the FortiGate unit - CLI

```
config system interface
  edit homenet_nw
    set ip 172.16.96.32 255.255.255.0
    set type switch
    set security-mode captive-portal
    set security-groups "Guest-group"
  end
config system interface
  edit homenet_nw
    set member "homenet_if" "internal"
  end
```

VLAN configuration

If your environment uses VLAN tagging, you assign the SSID to a specific VLAN in the CLI. For example, to assign the homenet_if interface to VLAN 100, enter:

```
config wireless-controller vap
  edit "homenet_if"
    set vlanid 100
  end
```

Additional configuration

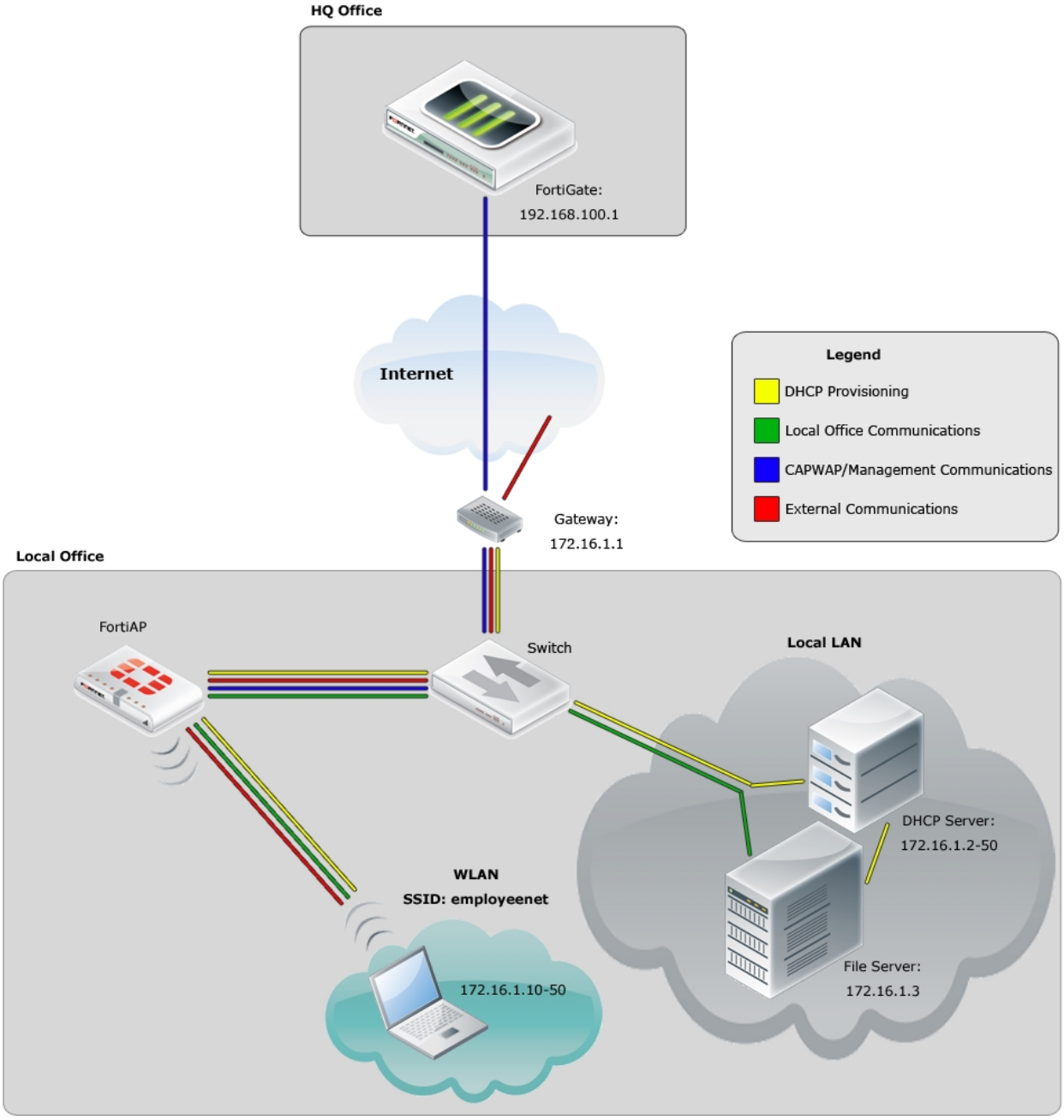
The configuration described above provides communication between WiFi and wired LAN users only. To provide access to other networks, create appropriate firewall policies between the software switch and other interfaces.

FortiAP local bridging (Private Cloud-Managed AP)

A FortiAP unit can provide WiFi access to a LAN, even when the wireless controller is located remotely. This configuration is useful for the following situations:

- Installations where the WiFI controller is remote and most of the traffic is local or uses the local Internet gateway
- Wireless-PCI compliance with remote WiFi controller
- Telecommuting, where the FortiAP unit has the WiFi controller IP address pre-configured and broadcasts the office SSID in the user's home or hotel room. In this case, data is sent in the wireless tunnel across the Internet to the office and you should enable encryption using DTLS.

Remotely-managed FortiAP providing WiFi access to local network



On the remote FortiGate wireless controller, the WiFi SSID is created with the **Bridge with FortiAP Interface** option selected. In this mode, no IP addresses are configured. The FortiAP unit's WiFi and Ethernet interfaces behave as a switch. WiFi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN.

The Local Bridge feature cannot be used in conjunction with Wireless Mesh features.

Block-Intra-SSID Traffic is not available in Bridge mode.

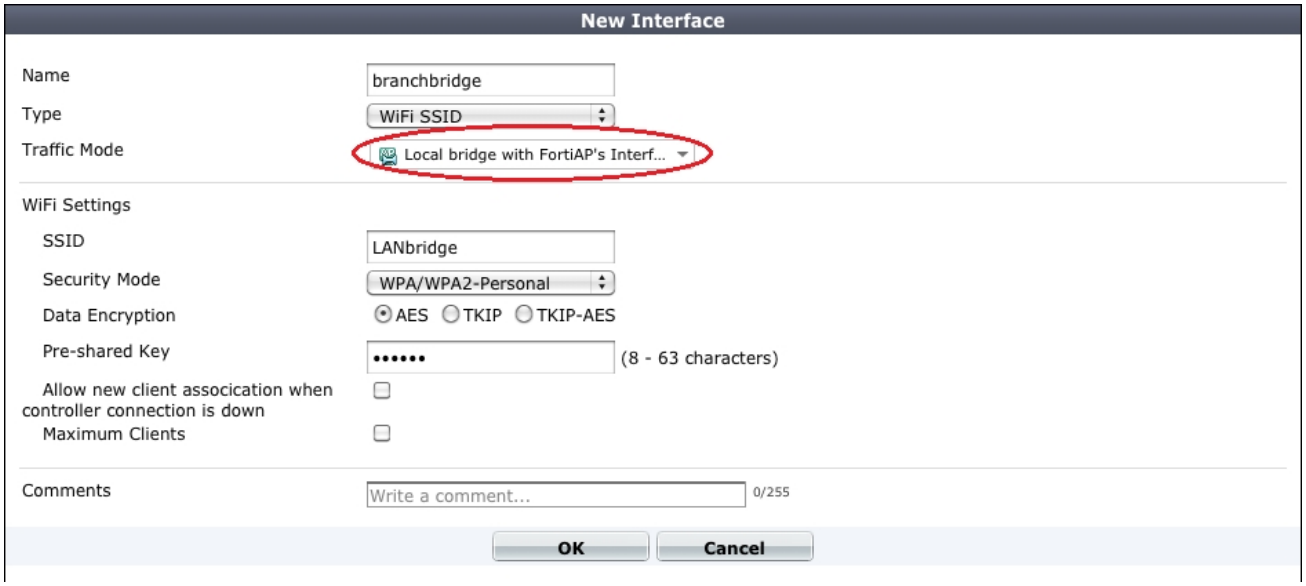
To configure a FortiAP local bridge - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Enter:

Interface name	A name for the new WiFi interface.
Traffic Mode	Local bridge with FortiAP's Interface
SSID	The SSID visible to users.
Security Mode **Data Encryption** **Preshared Key**	Configure security as you would for a regular WiFi network.

3. Select **OK**.
4. Go to **WiFi Controller > Managed Access Points > Managed FortiAP,** select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
   The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

SSID configured for Local Bridge operation



To configure a FortiAP local bridge - CLI

This example creates a WiFi interface “branchbridge” with SSID “LANbridge” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
   edit "branchbridge"
      set vdom "root"
      set ssid "LANbridge"
      set local-bridging enable
      set security wpa-personal
      set passphrase "Fortinet1"
   end
```

```
config wireless-controller wtp
   edit FAP22B3U11005354
      set admin enable
      set vaps "branchbridge"
   end
```

Continued FortiAP operation when WiFi controller connection is down

The wireless controller, or the connection to it, might occasionally become unavailable. During such an outage, clients already associated with a bridge mode FortiAP unit continue to have access to the WiFi and wired networks. Optionally, the FortiAP unit can also continue to authenticate users if the SSID meets these conditions:

- **Traffic Mode** is **Local bridge with FortiAP's Interface**.
  In this mode, the FortiAP unit does not send traffic back to the wireless controller.
- **Security Mode** is **WPA2 Personal**.
  These modes do not require the user database. In WPA2 Personal authentication, all clients use the same pre-shared key which is known to the FortiAP unit.
- **Allow New WiFi Client Connections When Controller is down** is enabled.
  This field is available only if the other conditions have been met.

The "LANbridge" SSID example would be configured like this in the CLI:

```
config wireless-controller vap
   edit "branchbridge"
      set vdom "root"
      set ssid "LANbridge"
      set local-bridging enable
      set security wpa-personal
      set passphrase "Fortinet1"
      set local-authentication enable
   end
```

Using bridged FortiAPs to increase scalability

The FortiGate wireless controller can support more FortiAP units in local bridge mode than in the normal mode. But this is only true if you configure some of your FortiAP units to operate in remote mode, which supports only local bridge mode SSIDs.

The Managed FortAP page (**WiFi Controller > Managed Devices > Managed FortiAP**) shows at the top right the current number of Managed FortiAPs and the maximum number that can be managed, "5/64" for example. The maximum number, however, is true only if all FortiAP units operate in remote mode. For more detailed information, consult the Maximum Values Table. For each FortiGate model, there are two maximum values for managed FortiAP units: the total number of FortiAPs and the number of FortiAPs that can operate in normal mode.

To configure FortiAP units for remote mode operation

1. Create at least one SSID with **Traffic Mode** set to **Local Bridge**.
2. Create a custom AP profile that includes only local bridge SSIDs.
3. Configure each managed FortiAP unit to use the custom AP profile. You also need to set the FortiAP unit's `wtp-mode` to `remote`, which is possible only in the CLI. The following example uses the CLI both to set `wtp-mode` and select the custom AP profile:

   ```
   config wireless-controller wtp
      edit FAP22B3U11005354
   ```

```
    set wtp-mode remote
    set wtp-profile 220B_bridge
end
```

Using Remote WLAN FortiAPs

Remote WLAN FortiAP models enable you to provide a pre-configured WiFi access point to a remote or traveling employee. Once plugged in at home or in a hotel room, the FortiAP automatically discovers the enterprise FortiGate WiFi controller over the Internet and broadcasts the same wireless SSID used in the corporate office. Communication between the WiFi controller and the FortiAP is secure, eliminating the need for a VPN.

Split tunneling

By default, all traffic from the remote FortiAP is sent to the FortiGate WiFi controller. If split tunneling is configured, only traffic destined for the corporate office networks is routed to the FortiGate unit. Other general Internet traffic is routed unencrypted through the local gateway. Split tunneling avoids loading the FortiGate unit with unnecessary traffic and allows access to local private networks at the FortiAP's location.

Note: Split tunneling in WiFi networks differs in implementation from split tunneling in VPN configurations.

By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the following CLI command:

```
config system global
   set gui-fortiap-split-tunneling enable
end
```

Split tunneling is configured in the FortiAP Profile and enabled in the SSID.

Configuring the FortiGate for remote FortiAPs

This section assumes that you have already defined SSIDs and now want to make them available to remote FortiAPs.

- Create FortiAP profiles for the Remote LAN FortiAP models
- If split tunneling will be used
  - enable Split Tunneling in the SSID
  - configure the split tunnel networks in the FortiAP profile

Creating FortiAP profiles

If you were not already using Remote LAN FortiAP models, you will need to create FortiAP profiles for them. In the FortiAP profile, you specify the SSIDs that the FortiAP will broadcast. For more information, see "Creating a FortiAP Profile" on page 817.

Configuring split tunneling - FortiGate GUI

Go to **WiFi Controller > WiFi Network > SSID** and edit your SSID. In the **WiFi Settings** section, enable **Split Tunneling**.

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the FortiAP Profile(s) that apply to the AP types used in the WiFi network. In **Split Tunneling Subnets**, enter a comma-separated list all of the destination

IP address ranges that should ***not*** be routed through the the FortiGate WiFi controller. Packets for these destinations will instead be routed through the remote gateway local to the FortiAP.

The list of split tunneling subnets includes public Internet destinations and private subnets local to the FortiAP. Split tunneling public Internet destinations reduces traffic through the FortiGate unit. Split tunneling local private subnets allows these networks to be accessible to the client behind the FortiAP. Otherwise, private network IP destinations are assumed to be behind the FortiGate WiFi controller.

Configuring split tunneling - FortiGate CLI

In this example, split tunneling is configured on the example-ssid WiFi network. On FortiAP model 21D, traffic destined for the 192.168.x.x range will not be routed through the FortiGate WiFi controller. This private IP address range is typically used as a LAN by home routers.

```
config wireless-controller vap
   edit example-ssid
      set split-tunneling enable
   end

config wireless-controller wtp-profile
   edit FAP21D-default
      set split-tunneling-acl-local-ap-subnet enable
      config split-tunneling-acl
         edit 1
            set dest-ip 192.168.0.0 255.255.0.0
         end
      end
```

To enter multiple subnets, create a split-tunneling-acl entry for each one.

Configuring the FortiAP units

Prior to providing a Remote WLAN FortiAP unit to an employee, you need to preconfigure the AP to connect to your FortiGate WiFi controller.

To pre-configure a FortiAP

1. Connect the FortiAP to the FortiGate unit.
2. Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and wait for the FortiAP to be listed. Click **Refresh** periodically to see the latest information. Note the **Connected Via** IP address.
3. Go to **System > Dashboard > Status**. In the CLI Console, log into the FortiAP CLI.
   For example, if the IP address is 192.168.1.4, enter:
   ```
   exec telnet 192.168.1.4
   ```
   Enter *admin* at the login prompt. By default, no password is set.
4. Enter the following commands to set the FortiGate WiFi controller IP address. This should be the FortiGate Internet-facing IP address, in this example 172.20.120.142.
   ```
   cfg -a AC_IPADDR_1=172.20.120.142
   cfg -c
   ```
5. Enter *exit* to log out of the FortiAP CLI.

Preauthorizing FortiAP units

By preauthorizing FortiAP units, you facilitate their automatic authorization on the network. Also, you can assign each unit a unique name, such as the employee's name, for easier tracking.

1. Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.
2. Enter the **Serial Number** of the FortiAP unit and give it a **Name**. Select the appropriate **FortiAP Profile**.
3. Click **OK**.

Repeat this process for each FortiAP.

Features for high-density deployments

High-density environments such as auditoriums, classrooms, and meeting rooms present a challenge to WiFi providers. When a large number of mobile devices try to connect to a WiFi network, difficulties arise because of the limited number of radio channels and interference between devices.

FortiOS and FortiAP devices provide several tools to mitigate the difficulties of high-density environments.

Broadcast packet suppression

Broadcast packets are sent at a low data rate in WiFi networks, consuming valuable air time. Some broadcast packets are unnecessary or even potentially detrimental to the network and should be suppressed.

ARP requests and replies could allow clients to discover each other's IP addresses. On most WiFi networks, intra-client communication is not allowed, so these ARP requests are of no use, but they occupy air time.

DHCP (upstream) should be allowed so that clients can request an IP address using DHCP.

DHCP (downstream) should be suppressed because it would allow a client to provide DHCP service to other clients. Only the AP should do this.

NetBIOS is a Microsoft Windows protocol for intra-application communication. Usually this is not required in high-density deployments.

IPv6 broadcast packets can be suppressed if your network uses IPv4 addressing.

You can configure broadcast packet suppression in the CLI. For example, to suppress ARP, downstream DHCP, NetBIOS, and IPv6 packets on the conf-net network, enter:

```
config wireless-controller vap
   edit conf_net
      set broadcast-suppress arp-known arp-unknown arp-reply dhcp-down netbios-ns netbios-
          ds ipv6
   end
```

Multicast to unicast conversion

Multicast data such as streaming audio or video are sent at a low data rate in WiFi networks. This causes them to occupy considerable air time. FortiOS provides a multicast enhancement option that converts multicast streams to unicast. A unicast stream is sent to each client at high data rate that makes more efficient use of air time. You can configure multicast-to-unicast conversion in the CLI:

```
config wireless-controller vap
   edit <vap_name>
      set multicast-enhance enable
   end
```

Ignore weak or distant clients

Clients beyond the intended coverage area can have some impact on your high-density network. Your APs will respond to these clients' probe signals, consuming valuable air time. You can configure your WiFi network to ignore weak signals that most likely come from beyond the intended coverage area. The settings are available in the CLI:

```
config wireless-controller vap
   edit <vap_name>
      set probe-resp-suppression enable
      set probe-resp-threshold <level_int>
   end
```

vap_name is the SSID name.

probe-resp-threshold is the signal strength in dBm below which the client is ignored. The range is -95 to -20dBm. The default level is -80dBm.

Turn off 802.11b protocol

By disabling support for the obsolete 802.11b protocol, you can reduce the air time that beacons and management frames occupy. These signals will now be sent at a minimum of 6Mbps, instead of 1Mbps. You can set this for each radio in the FortiAP profile, using the CLI:

```
config wireless-controller wtp-profile
   edit <name_string>
      config radio-1
         set powersave-optimize no-11b-rate
      end
```

Limit power

High-density deployments usually cover a small area that has many clients. Maximum AP signal power is usually not required. Reducing the power reduces interference between APs. Fortinet recommends that you use FortiAP automatic power control. You can set this in the FortiAP profile.

1. Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile for your AP model.
2. For each radio, enable **Auto TX Power Control** and set the **TX Power Low** and **TX Power High** levels. The default range of 10 to 17dBm is recommended.

Use frequency band load-balancing

In a high-density environment is important to make the best use of the two WiFi bands, 2.4GHz and 5GHz. The 5GHz band has more non-overlapping channels and receives less interference from non-WiFi devices, but not all devices support it. Clients that are capable of 5GHz operation should be encouraged to use 5GHz rather than the 2.4GHz band.

To load-balance the WiFi bands, you enable Frequency Handoff in the FortiAP profile. In the FortiGate web-based manager, go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the relevant profile. Or, you can use the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      config radio-1
         set frequency-handoff enable
      end
```

The FortiGate wireless controller continuously performs a scan of all clients in the area and records their signal strength (RSSI) on each band. When Frequency Handoff is enabled, the AP does not reply to clients on the 2.4GHz band that have sufficient signal strength on the 5GHz band. These clients can associate only on the 5GHz band. Devices that support only 2.4GHz receive replies and associate with the AP on the 2.4GHz band.

Setting the handoff RSSI threshold

The FortiAP applies load balancing to a client only if the client has a sufficient signal level on 5GHz. The minimum signal strength threshold is set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      set handoff-rssi 25
   end
```

`handoff-rssi` has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

AP load balancing

The performance of an AP is degraded if it attempts to serve too many clients. In high-density environments, multiple access points are deployed with some overlap in their coverage areas. The WiFi controller can manage the association of new clients with APs to prevent overloading.

To load-balance between APs, enable AP Handoff in the FortiAP profile. In the FortiGate web-based manager, go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the relevant profile. Or, you can use the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      config radio-1
         set ap-handoff enable
      end
```

When an AP exceeds the threshold (the default is 30 clients), the overloaded AP does not reply to a new client that has a sufficient signal at another AP.

Setting the AP load balance threshold

The thresholds for AP handoff are set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      set handoff-sta-thresh 30
      set handoff-rssi 25
   end
```

`handoff-sta-thresh` sets the number of clients at which AP load balancing begins. It has a range of 5 to 35.

`handoff-rssi` Sets the minimum signal strength that a new client must have at an alternate AP for the overloaded AP to ignore the client. It has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

Application rate-limiting

To prevent particular application types from consuming too much bandwidth, you can use the FortiOS Application Control feature.

1. Go to **Security Profiles > Application Control**.
   You can use the default profile or create a new one.
2. Click the category, select **Traffic Shaping** and then select the priority for the category.
   Repeat for each category to be controlled.
3. Select **Apply**.
4. Go to **Policy & Objects > Policy > IPv4** and edit your WiFi security policy.
5. In **Security Profiles**, set **Application Control** ON and select the security profile that you edited.
6. Select **OK**.

Protecting the WiFi Network

Wireless IDS
WiFi data channel encryption

Wireless IDS

The FortiGate Wireless Intrusion Detection System (WIDS) monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected the FortiGate unit records a log message.

You can create a WIDS profile to enable these types of intrusion detection:

- Asleap Attack—ASLEAP is a tool used to perform attacks against LEAP authentication.
- Association Frame Flooding—A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
- Authentication Frame Flooding—A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
- Broadcasting De-authentication—This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-athenticate, then re-authenticate with their AP.
- EAPOL Packet Flooding—Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.
- Invalid MAC OUI—Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
- Long Duration Attack—To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
- Null SSID Probe Response—When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
- Spoofed De-authentication—Spoofed de-authentication frames form the basis for most denial of service attacks.
- Weak WEP IV Detection—A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
- Wireless Bridge—WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

You can enable wireless IDS by selecting a WIDS Profile in your FortiAP profile.

To create a WIDS Profile

1. Go to **WiFi Controller > WiFi Network > WIDS Profile**.
2. Select a profile to edit or select **Create New**.
3. Select the types of intrusion to protect against.
   By default, all types are selected.
4. Select **Apply**.

You can also configure a WIDS profile in the CLI using the `config wireless-controller wids-profile` command.

Rogue AP detection

The WIDS profile includes settings for detection of unauthorized (rogue) access points in your wireless network. For more information, see Wireless network monitoring on page 870.

WiFi data channel encryption

Optionally, you can apply DTLS encryption to the data channel between the wireless controller and FortiAP units. This enhances security.

There are data channel encryption settings on both the FortiGate unit and the FortiAP units. At both ends, you can enable Clear Text, DTLS encryption, or both. The settings must agree or the FortiAP unit will not be able to join the WiFi network. By default, both Clear Text and DTLS-encrypted communication are enabled on the FortiAP unit, allowing the FortiGate setting to determine whether data channel encryption is used. If the FortiGate unit also enables both Clear Text and DTLS, Clear Text is used.

Data channel encryption settings are located in the Custom AP profile. If you use Automatic profile, only Clear Text is supported.

Data channel encryption is software-based and can affect performance. Verify that the system meets your performance requirements with encryption enabled.

Configuring encryption on the FortiGate unit

You can use the CLI to configure data channel encryption.

Enabling encryption

In the CLI, the `wireless wtp-profile` command contains a new field, `dtls-policy`, with options `clear-text` and `dtls-enabled`. To enable encryption in profile1 for example, enter:

```
config wireless-controller wtp-profile
   edit profile1
      set dtls-policy dtls-enabled
   end
```

Configuring encryption on the FortiAP unit

The FortiAP unit has its own settings for data channel encryption.

Enabling CAPWAP encryption - FortiAP web-based manager

1. On the **System Information** page, in **WTP Configuration > AC Data Channel Security**, select one of:
   - Clear Text
   - DTLS Enabled
   - Clear Text or DTLS Enabled (default)
2. Select **Apply**.

Enabling encryption - FortiAP CLI

You can set the data channel encryption using the AC_DATA_CHAN_SEC variable: 0 is Clear Text, 1 is DTLS Enabled, 2 (the default) is Clear Text or DTLS Enabled.

For example, to set security to DTLS and then save the setting, enter

```
cfg -a AC_DATA_CHAN_SEC=1
cfg -c
```

Wireless network monitoring

You can monitor both your wireless clients and other wireless networks that are available in your coverage area.

Monitoring wireless clients
Monitoring rogue APs
Suppressing rogue APs
Monitoring wireless network health

Monitoring wireless clients

To view connected clients on a FortiWiFi unit

1. Go to **WiFi Controller > Monitor > Client Monitor.**
   The following information is displayed:

SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit to which the client connected.
User	User name
IP	The IP address assigned to the wireless client.
Device	
Auth	The type of authentication used.
Channel	WiFi radio channel in use.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength / Noise	The signal-to-noise ratio in deciBels calculated from signal strength and noise level.
Signal Strength	
Association Time	How long the client has been connected to this access point.

Results can be filtered. Select the filter icon on the column you want to filter. Enter the values to include or select NOT if you want to exclude the specified values.

Monitoring rogue APs

The access point radio equipment can scan for other available access points, either as a dedicated monitor or in idle periods during AP operation.

Discovered access points are listed in the **Rogue AP Monitor** list. You can then mark them as either Accepted or Rogue access points. This designation helps you to track access points. It does not affect anyone's ability to use these access points.

It is also possible to suppress rogue APs. See Monitoring rogue APs on page 870.

On-wire rogue AP detection technique

Other APs that are available in the same area as your own APs are not necessarily rogues. A neighboring AP that has no connection to your network might cause interference, but it is not a security threat. A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access. When rogue AP detection is enabled, the **On-wire** column in the **Rogue AP Monitor** list shows a green up-arrow on detected rogues.

Rogue AP monitoring of WiFi client traffic builds a table of WiFi clients and the Access Points that they are communicating through. The FortiGate unit also builds a table of MAC addresses that it sees on the LAN. The FortiGate unit's on-wire correlation engine constantly compares the MAC addresses seen on the LAN to the MAC addresses seen on the WiFi network.

There are two methods of Rogue AP on-wire detection operating simultaneously: Exact MAC address match and MAC adjacency.

Exact MAC address match

If the same MAC address is seen on the LAN and on the WiFi network, this means that the wireless client is connected to the LAN. If the AP that the client is using is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue. This scheme works for non-NAT rogue APs.

MAC adjacency

If an access point is also a router, it applies NAT to WiFi packets. This can make rogue detection more difficult. However, an AP's WiFi interface MAC address is usually in the same range as its wired MAC address. So, the MAC adjacency rogue detection method matches LAN and WiFi network MAC addresses that are within a defined numerical distance of each other. By default, the MAC adjacency value is 7. If the AP for these matching MAC addresses is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue.

Limitations

On-wire rogue detection has some limitations. There must be at least one WiFi client connected to the suspect AP and continuously sending traffic. If the suspect AP is a router, its WiFi MAC address must be very similar to its Ethernet port MAC address.

Logging

Information about detected rogue APs is logged and uploaded to your FortiAnalyzer unit, if you have one. By default, rogue APs generate an alert level log, unknown APs generate a warning level log. This log information can help you with PCI-DSS compliance requirements.

Rogue AP scanning as a background activity

Each WiFi radio can perform monitoring of radio channels in its operating band while acting as an AP. It does this by briefly switching from AP to monitoring mode. By default, a scan period starts every 300 seconds. Each second a different channel is monitored for 20ms until all channels have been checked.

During heavy AP traffic, it is possible for Spectrum Analysis background scanning to cause lost packets when the radio switches to monitoring. To reduce the probability of lost packets, you can set the CLI `ap-bgscan-idle`

field to delay the switch to monitoring until the AP has been idle for a specified period. This means that heavy AP traffic may slow background scanning.

The following CLI example configures default background rogue scanning operation except that it sets `ap-bgscan-idle` to require 100ms of AP inactivity before scanning the next channel.

```
config wireless-controller wtp-profile
   edit ourprofile
      config radio-1
         set wids-profile ourwidsprofile
         set spectrum-analysis enable
      end
   end
config wireless-controller wids-profile
   edit ourwidsprofile
      set ap-scan enable
      set rogue-scan enable
      set ap-bgscan-period 300
      set ap-bgscan-intv 1
      set ap-bgscan-duration 20
      set ap-bgscan-idle 100
   end
```

Configuring rogue scanning

All APs using the same FortiAP Profile share the same rogue scanning settings, unless override is configured.

To enable rogue AP scanning with on-wire detection - web-based manager

1. Go to **WiFi Controller > WiFi Network > WIDS Profiles**.
   On some models, the menu is **WiFi & Switch Controller**.
2. Select an existing WIDS Profile and edit it, or select **Create New**.
3. Make sure that **Enable Rogue AP Detection** is selected.
4. Select **Enable On-Wire Rogue AP Detection.**
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Select **OK**.

To enable the rogue AP scanning feature in a custom AP profile - CLI

```
config wireless-controller wids-profile
   edit FAP220B-default
      set ap-scan enable
      set rogue-scan enable
   end
```

Exempting an AP from rogue scanning

By default, if Rogue AP Detection is enabled, it is enabled on all managed FortiAP units. Optionally, you can exempt an AP from scanning. You should be careful about doing this if your organization must perform scanning to meet PCI-DSS requirements.

To exempt an AP from rogue scanning - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.
2. Select which AP to edit.
3. In **Wireless Settings**, enable **Override Settings**.
4. Select **Do not participate in Rogue AP Scanning** and then select **OK**.

To exempt an AP from rogue scanning - CLI

This example shows how to exempt access point AP1 from rogue scanning.

```
config wireless-controller wtp
   edit AP1
      set override-profile enable
      set ap-scan disable
   end
```

MAC adjacency

You can adjust the maximum WiFi to Ethernet MAC difference used when determining whether an suspect AP is a rogue.

To adjust MAC adjacency

For example, to change the adjacency to 8, enter

```
config wireless-controller global
   set rogue-scan-mac-adjacency 8
end
```

Using the Rogue AP Monitor

Go to **WiFi Controller > Monitor > Rogue AP Monitor** to view the list of other wireless access points that are receivable at your location.

Information Columns Actual columns displayed depends on **Column Settings.**	
State	Rogue AP — Use this status for unauthorized APs that **On-wire** status indicates are attached to your wired networks. Accepted AP — Use this status for APs that are an authorized part of your network or are neighboring APs that are not a security threat. To see accepted APs in the list, select **Show Accepted**. Unclassified — This is the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as Rogue or Accepted.
Online Status	Active AP Inactive AP Active ad-hoc WiFi device Inactive ad-hoc WiFi device
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the Wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP. Mouse over the symbol to view the signal-to-noise ratio.
Detected By	The name or serial number of the AP unit that detected the signal.
On-wire	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. A red down-arrow indicates AP is not a suspected rogue.
First Seen	How long ago this AP was first detected.
Last Seen	How long ago this AP was last detected.
Rate	Data rate in bps.

To change the Online Status of an AP, right-click it and select Mark Accepted or Mark Rogue.

Suppressing rogue APs

In addition to monitoring rogue APs, you can actively prevent your users from connecting to them. When suppression is activated against an AP, the FortiGate WiFi controller sends deauthentication messages to the rogue AP's clients, posing as the rogue AP, and also sends deauthentication messages to the rogue AP, posing as its clients. This is done using the monitoring radio.

Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.

To enable rogue AP suppression, you must enable monitoring of rogue APs with the on-wire detection technique. See "Monitoring rogue APs". The monitoring radio must be in the Dedicated Monitor mode.

To activate AP suppression against a rogue AP

1. Go to **WiFi Controller > Monitor > Rogue AP Monitor.**
2. When you see an AP listed that is a rogue detected "on-wire", select it and then select **Mark > Mark Rogue**.
3. To suppress an AP that is marked as a rogue, select it and then select **Suppress AP**.

To deactivate AP suppression

1. Go to **WiFi Controller > Monitor > Rogue AP Monitor.**
2. Select the suppressed rogue AP and then select **Suppress AP > Unsuppress AP**.

Monitoring wireless network health

The Wireless Health Dashboard provides a comprehensive view of the health of your network's wireless infrastructure. The dashboard includes widgets to display

- AP Status - Active, Down or missing, up for over 24 hours, rebooted in past 24 hours
- Client Count Over Time - viewable for past hour, day, or 30 days
- Top Client Count Per-AP - separate widgets for 2.4GHz and 5GHz bands
- Top Wireless Interference - separate widgets for 2.4GHz and 5GHz bands, requires spectrum analysis to be enabled on the radios
- Login Failures Information

To view the Wireless Health dashboard, go to **WiFi Controller > Monitor > Wireless Health**.

Configuring wireless network clients

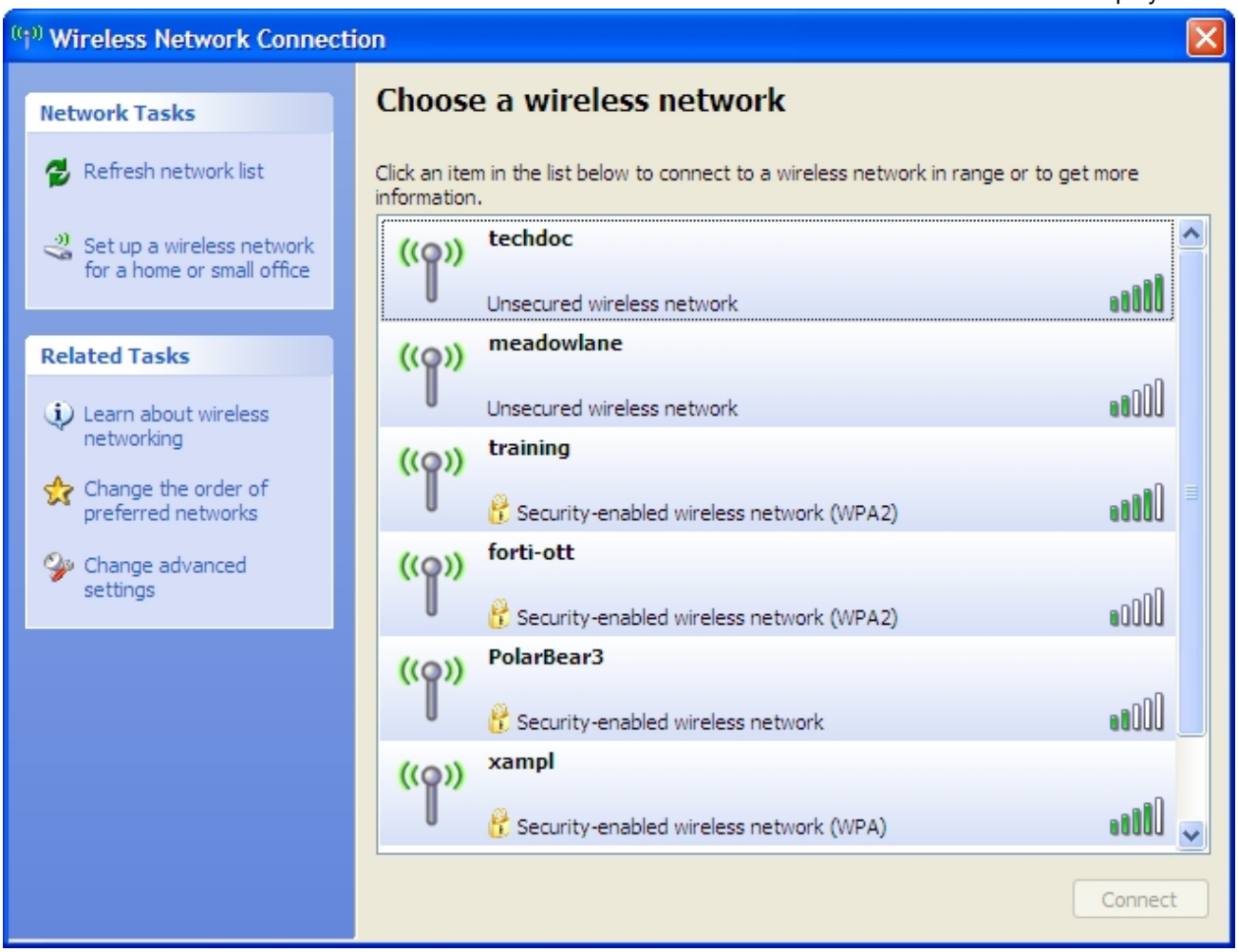
This chapter shows how to configure typical wireless network clients to connect to a wireless network with WPA-Enterprise security.

Windows XP client
Windows 7 client
Mac OS client
Linux client
Troubleshooting

Windows XP client

To configure the WPA-Enterprise network connection

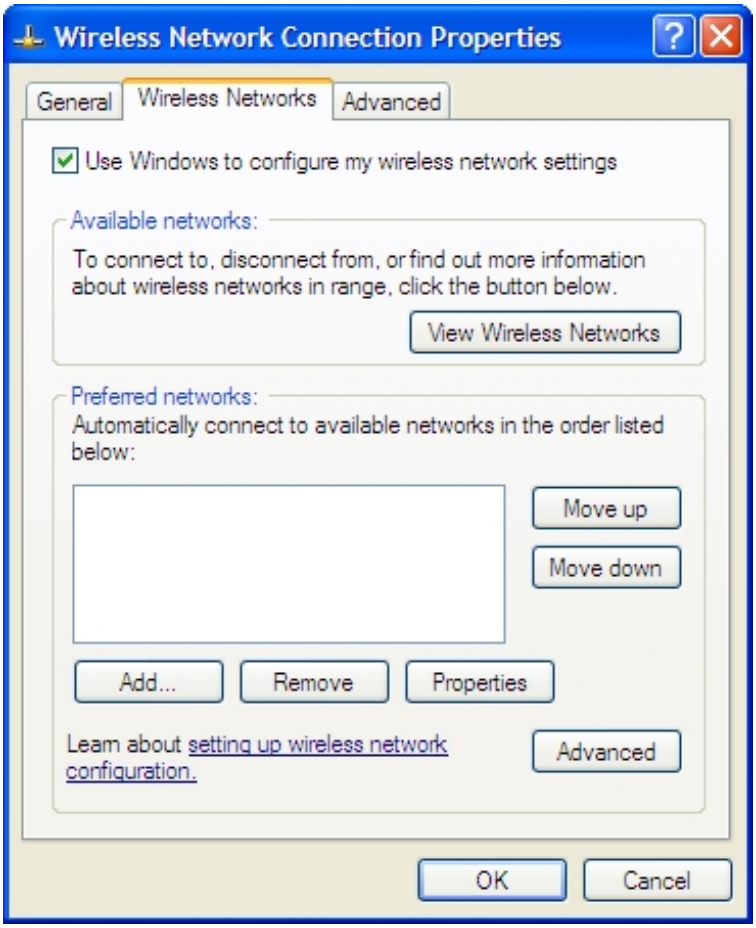
1. In the Windows Start menu, go to **Control Panel > Network Connections > Wireless Network Connection** or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.



If you are already connected to another wireless network, the Connection Status window displays. Select **View Wireless Networks** on the **General** tab to view the list.

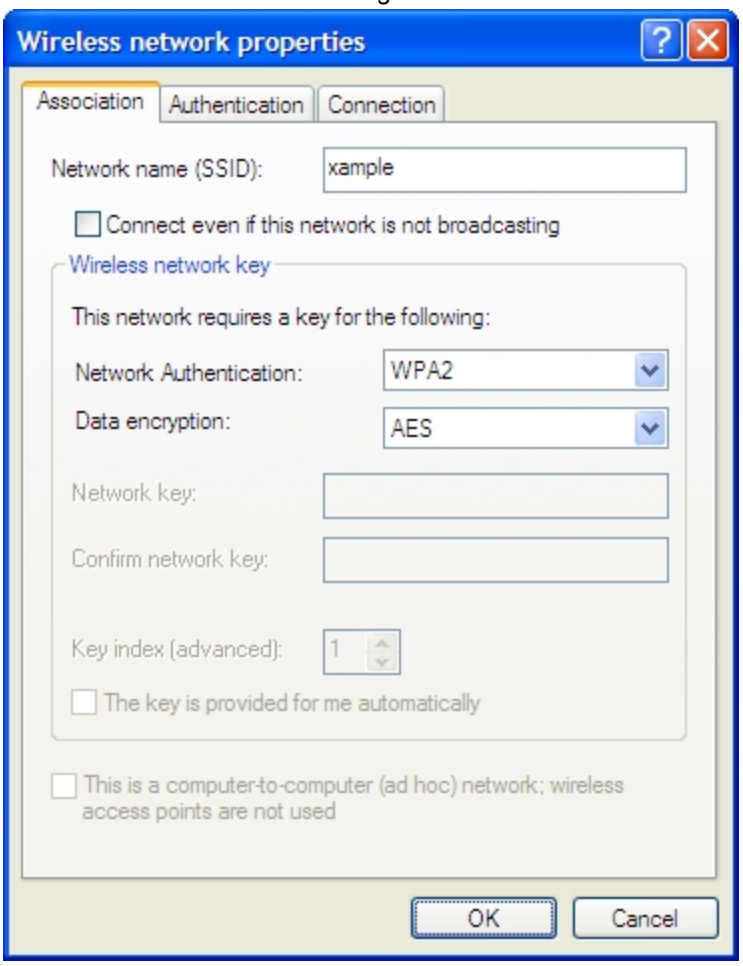
If the network broadcasts its SSID, it is listed. But do not try to connect until you have completed the configuration step below. Because the network doesn't use the Windows XP default security configuration, configure the client's network settings manually before trying to connect.

2. You can configure the WPA-Enterprise network to be accessible from the **View Wireless Networks** window even if it does not broadcast its SSID.
3. Select **Change Advanced Settings** and then select the **Wireless Networks** tab.



Any existing networks that you have already configured are listed in the **Preferred Networks** list.

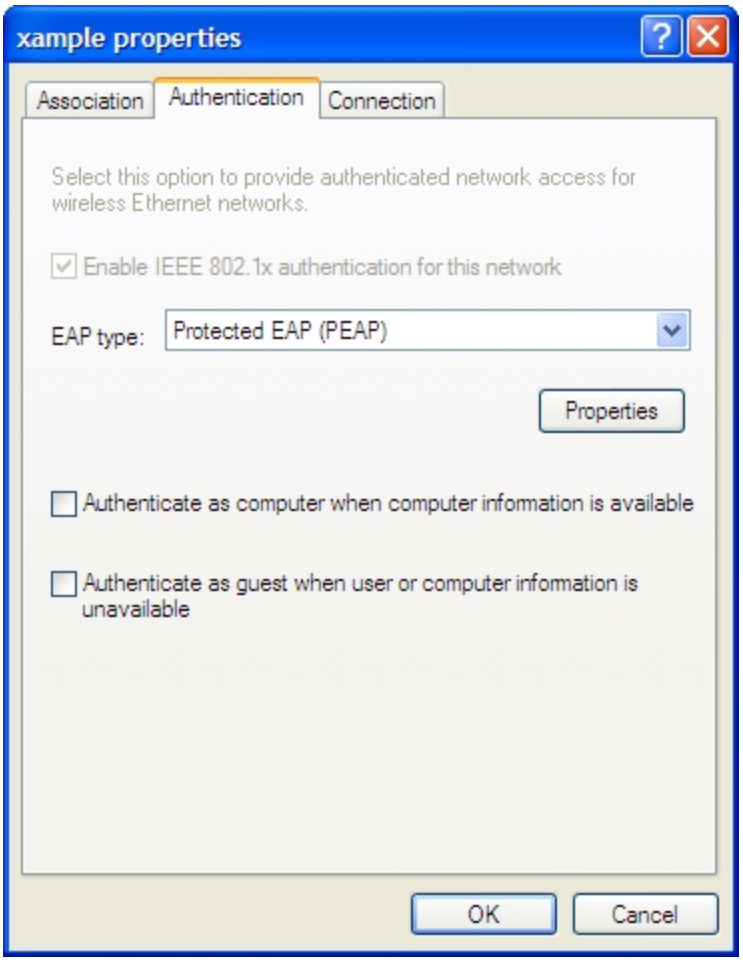
4. Select **Add** and enter the following information:



Network Name (SSID)	The SSID for your wireless network
Network Authentication	WPA2
Data Encryption	AES

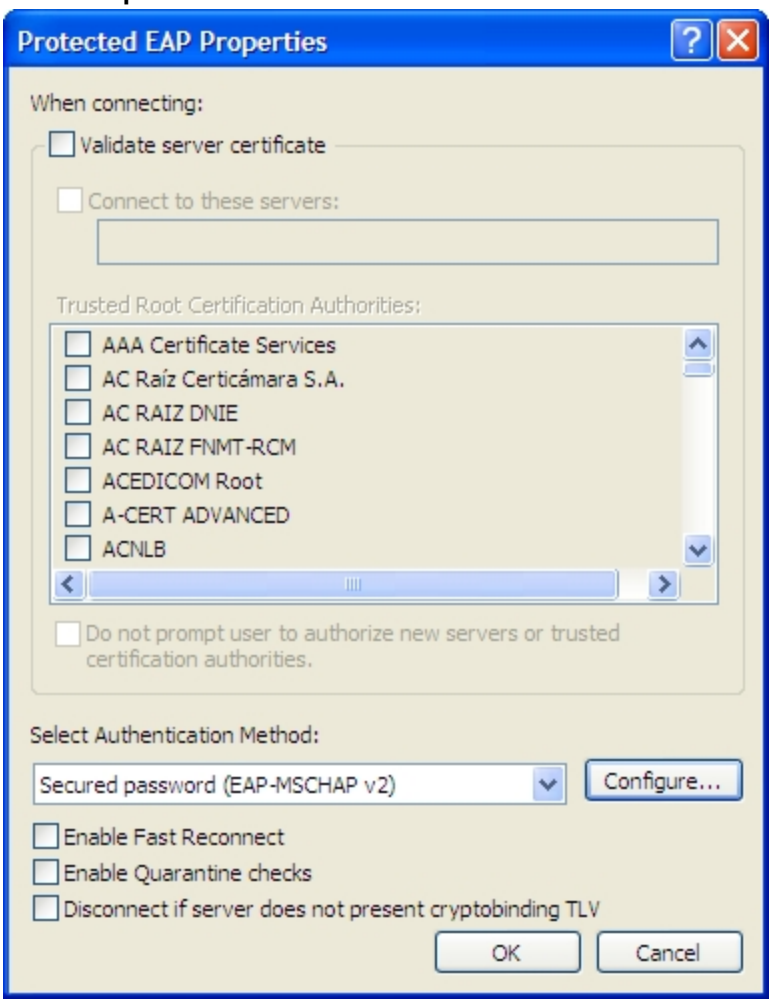
5. If this wireless network does not broadcast its SSID, select **Connect even if this network is not broadcasting** so that the network will appear in the **View Wireless Networks** list.

6. Select the **Authentication** tab.



7. In **EAP Type**, select **Protected EAP (PEAP)**.
8. Make sure that the other two authentication options are not selected.

9. Select **Properties**.



10. Make sure that **Validate server_certificate** is selected.
11. Select the server certificate UTN-USERFirst-Hardware.
12. In **Select Authentication Method**, select **Secured Password (EAP-MSCHAPv2)**.
13. Ensure that the remaining options are not selected.
14. Select **Configure**.

15. If your wireless network credentials are the same as your Windows logon credentials, select **Automatically use my Windows logon name and password**. Otherwise, make sure that this option is not selected.
16. Select **OK**. Repeat until you have closed all of the **Wireless Network Connection Properties** windows.

To connect to the WPA-Enterprise wireless network

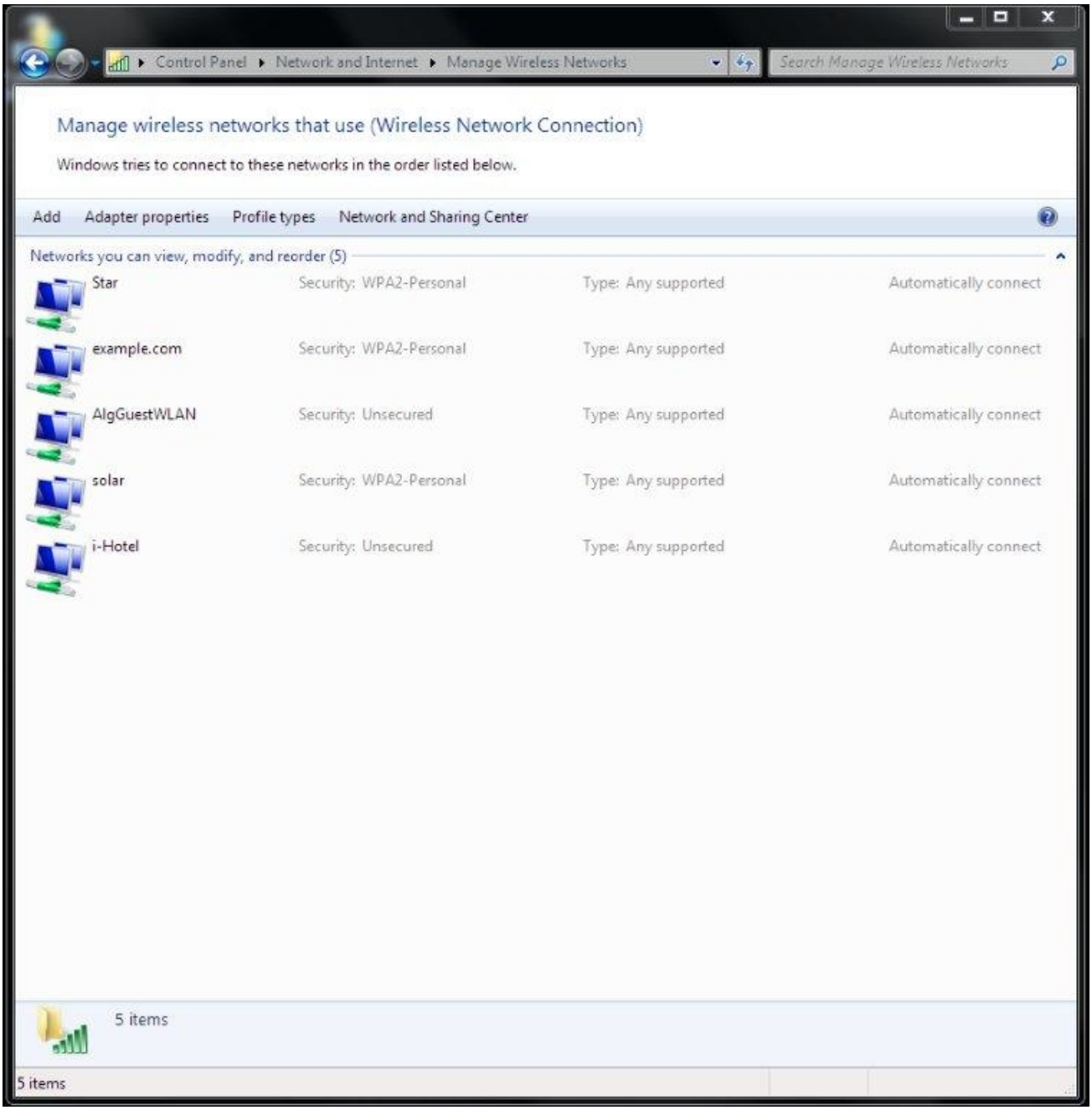
1. Select the wireless network icon in the Notification area of the Taskbar.
2. In the **View Wireless Networks** list, select the network you just added and then select **Connect**.
   You might need to log off of your current wireless network and refresh the list.
3. When the following popup displays, click on it.

4. In the **Enter Credentials** window, enter your wireless network **User name**, **Password**, and **Logon domain** (if applicable). Then, select **OK**.

In future, Windows will automatically send your credentials when you log on to this network.

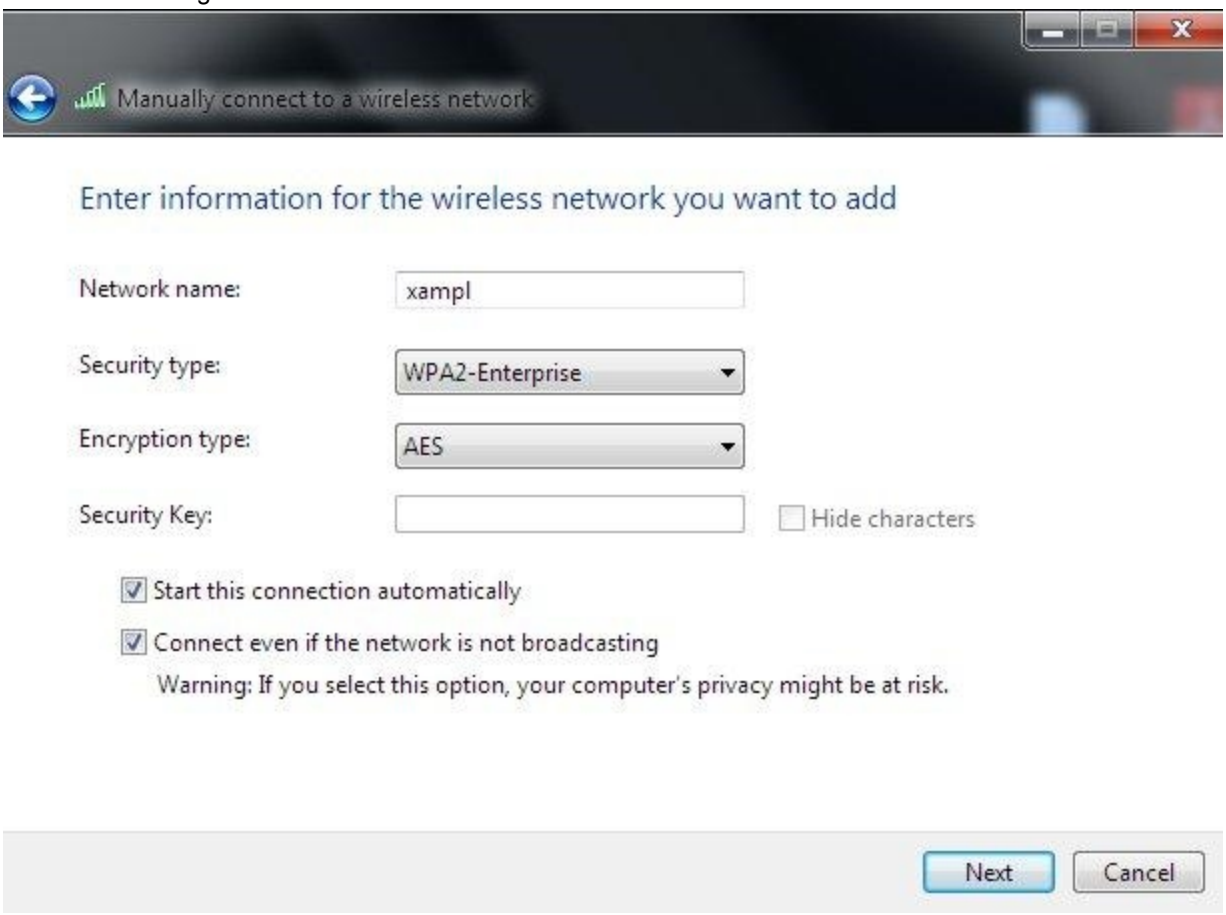
Windows 7 client

1. In the Windows Start menu, go to **Control Panel > Network and Internet > Network and Sharing Center > Manage Wireless Networks** or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.



2. Do one of the following:
   - If the wireless network is listed (it broadcasts its SSID), select it from the list.
   - Select **Add** > **Manually create a network profile**.

3. Enter the following information and select **Next**.



Network name	Enter the SSID of the wireless network. (Required only if you selected **Add**.)
Security type	WPA2-Enterprise
Encryption type	AES
Start this connection automatically	Select
Connect even if the network is not broadcasting.	Select

The Wireless Network icon will display a popup requesting that you click to enter credentials for the network. Click on the popup notification.

4. In the **Enter Credentials** window, enter your wireless network **User name**, **Password**, and **Logon domain** (if applicable). Then, select **OK**.
5. Select **Change connection settings**.
6. On the **Connection** tab, select **Connect automatically when this network is in range**.
7. On the **Security** tab, select the Microsoft PEAP authentication method and then select **Settings**.
8. Make sure that **Validate server_certificate** is selected.

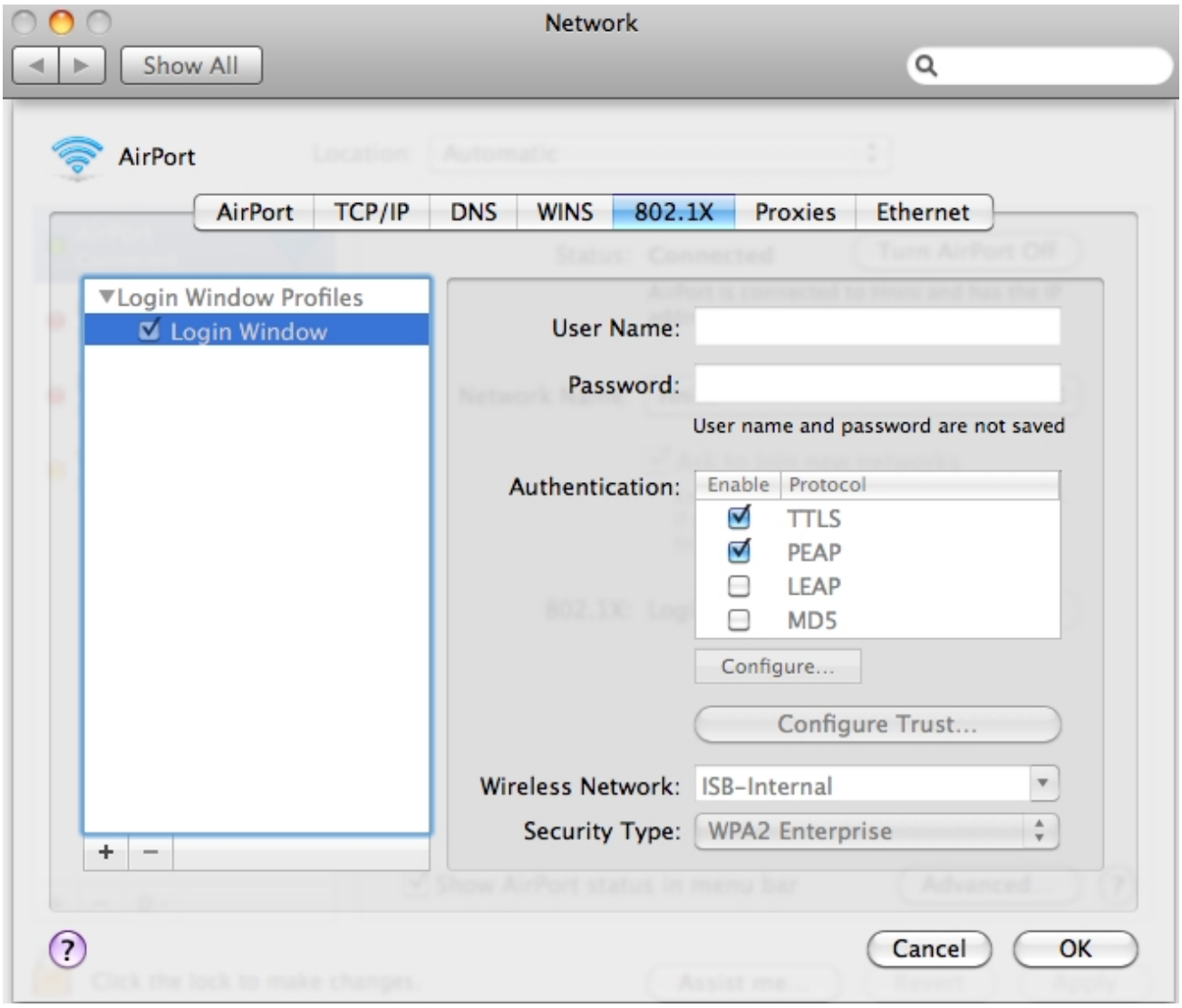
9. Select the server certificate UTN-USERFirst-Hardware.
10. In **Select Authentication Method**, select **Secured Password (EAP-MSCHAPv2)**.
11. Select **Configure**.

12. If your wireless network credentials are the same as your Windows logon credentials, select **Automatically use my Windows logon name and password**. Otherwise, make sure that this option is not selected.
13. Ensure that the remaining options are not selected.
14. Select **OK**. Repeat until you have closed all of the **Wireless Network Properties** windows.

Mac OS client

To configure network preferences

1. Right-click the **AirPort** icon in the toolbar and select **Open Network Preferences**.
2. Select **Advanced** and then select the **802.1X** tab.



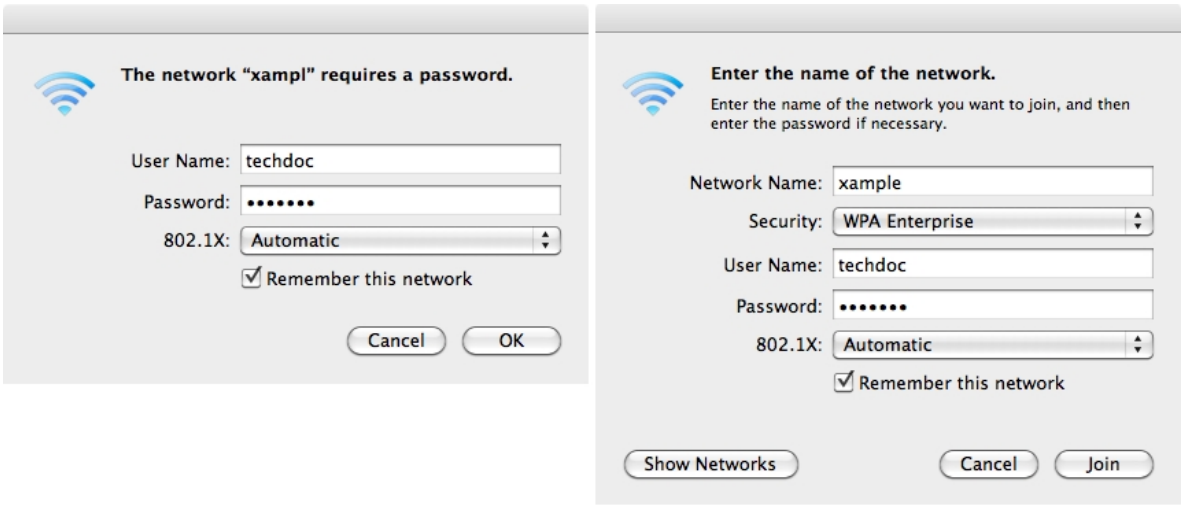
3. If there are no Login Window Profiles in the left column, select the + button and then select **Add Login Window Profile**.
4. Select the Login Window Profile and then make sure that both TTLS and PEAP are selected in **Authentication**.

To configure the WPA-Enterprise network connection

1. Select the **AirPort** icon in the toolbar.
2. Do one of the following:

- If the network is listed, select the network from the list.
- Select **Connect to Other Network**.

One of the following windows opens, depending on your selection.



3. Enter the following information and select **OK** or **Join**:

Network name	Enter the SSID of your wireless network. (Other network only)
Wireless Security	WPA Enterprise
802.1X	Automatic
Username **Password**	Enter your logon credentials for the wireless network.
Remember this network	Select.

You are connected to the wireless network.

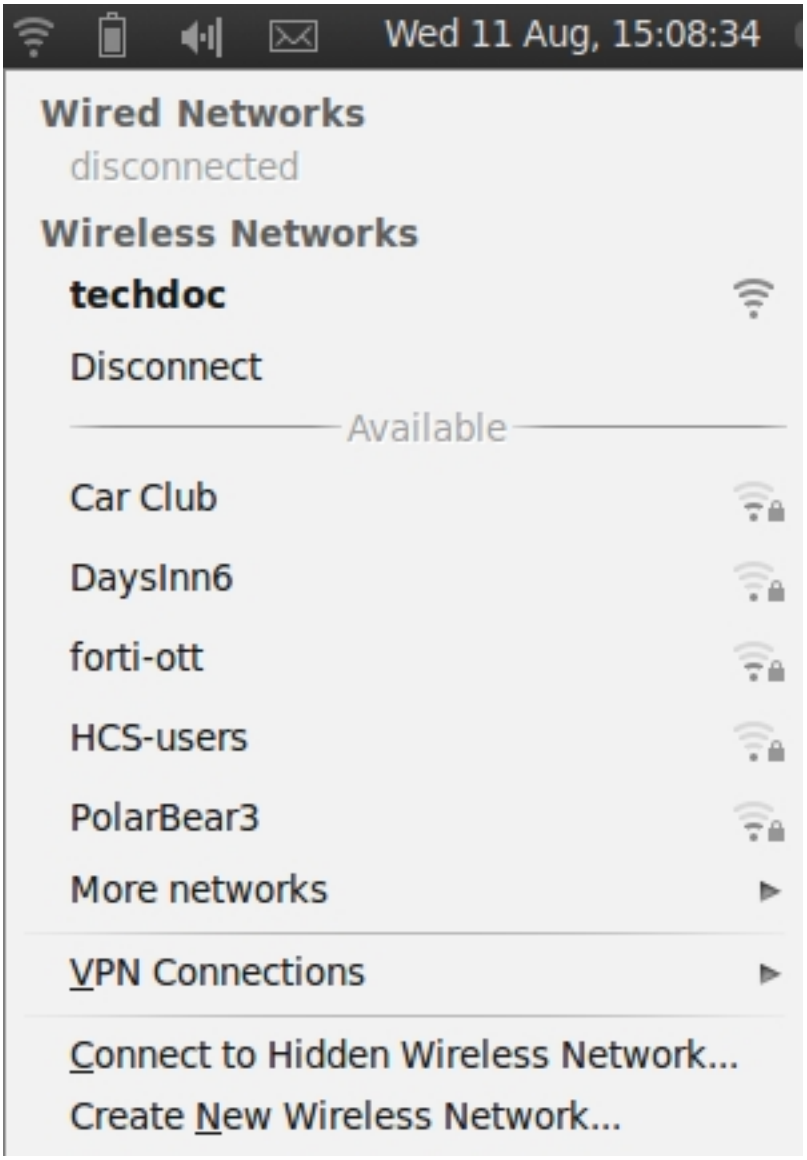
Mac OS supports only PEAP with MSCHAPv2 authentication and therefore can authenticate only to a RADIUS server, not an LDAP or TACACS+ server

Linux client

This example is based on the Ubuntu 10.04 Linux wireless client.

To connect to a WPA-Enterprise network

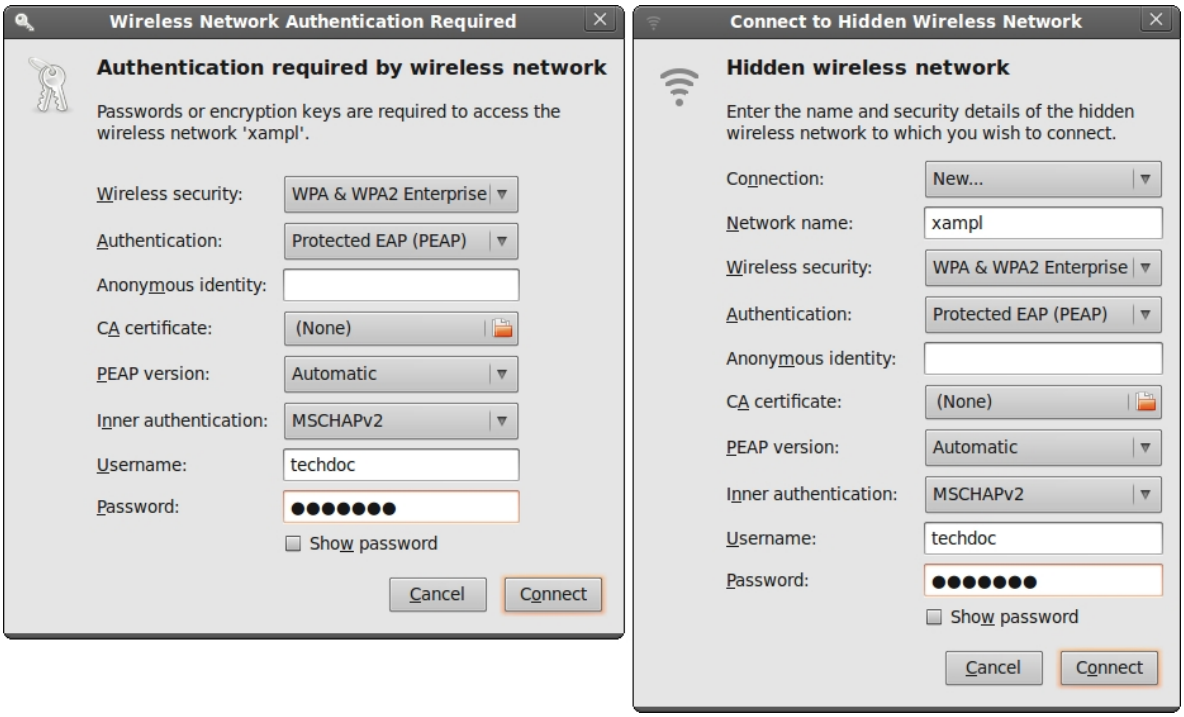
1. Select the Network Manager icon to view the Wireless Networks menu.



   Wireless networks that broadcast their SSID are listed in the **Available** section of the menu. If the list is long, it is continued in the **More Networks** submenu.

2. Do one of the following:
   - Select the network from the list (also check **More Networks**).
   - Select **Connect to Hidden Wireless Network**.

   One of the following windows opens, depending on your selection.



3. Enter the following information:

Connection	Leave as **New**. (Hidden network only)
Network name	Enter the SSID of your wireless network. (Hidden network only)
Wireless Security	WPA & WPA2 Enterprise
Authentication	Protected EAP (PEAP) for RADIUS-based authentication Tunneled TLS for TACACS+ or LDAP-based authentication
Anonymous identity	This is not required.
CA Certificate	If you want to validate the AP's certificate, select the UTN-USERFirst-Hardware root certificate. The default location for the certificate is /usr/share/ca-certificates/mozilla/.
PEAP version	Automatic (applies only to PEAP)
Inner authentication	MSCHAPv2 for RADIUS-based authentication PAP or CHAP for TACACS+ or LDAP-based authentication
Username **Password**	Enter your logon credentials for the wireless network.

4. If you did not select a CA Certificate above, you are asked to do so. Select Ignore.

5. Select **Connect.** You are connected to the wireless network.

To connect to a WPA-Enterprise network

1. Select the Network Manager icon to view the Wireless Networks menu.
2. Select the network from the list (also check **More Networks**).
   If your network is not listed (but was configured), select **Connect to Hidden Wireless Network**, select your network from the Connection drop-down list, and then select **Connect**.

Troubleshooting

Using tools provided in your operating system, you can find the source of common wireless networking problems.

Checking that client received IP address and DNS server information

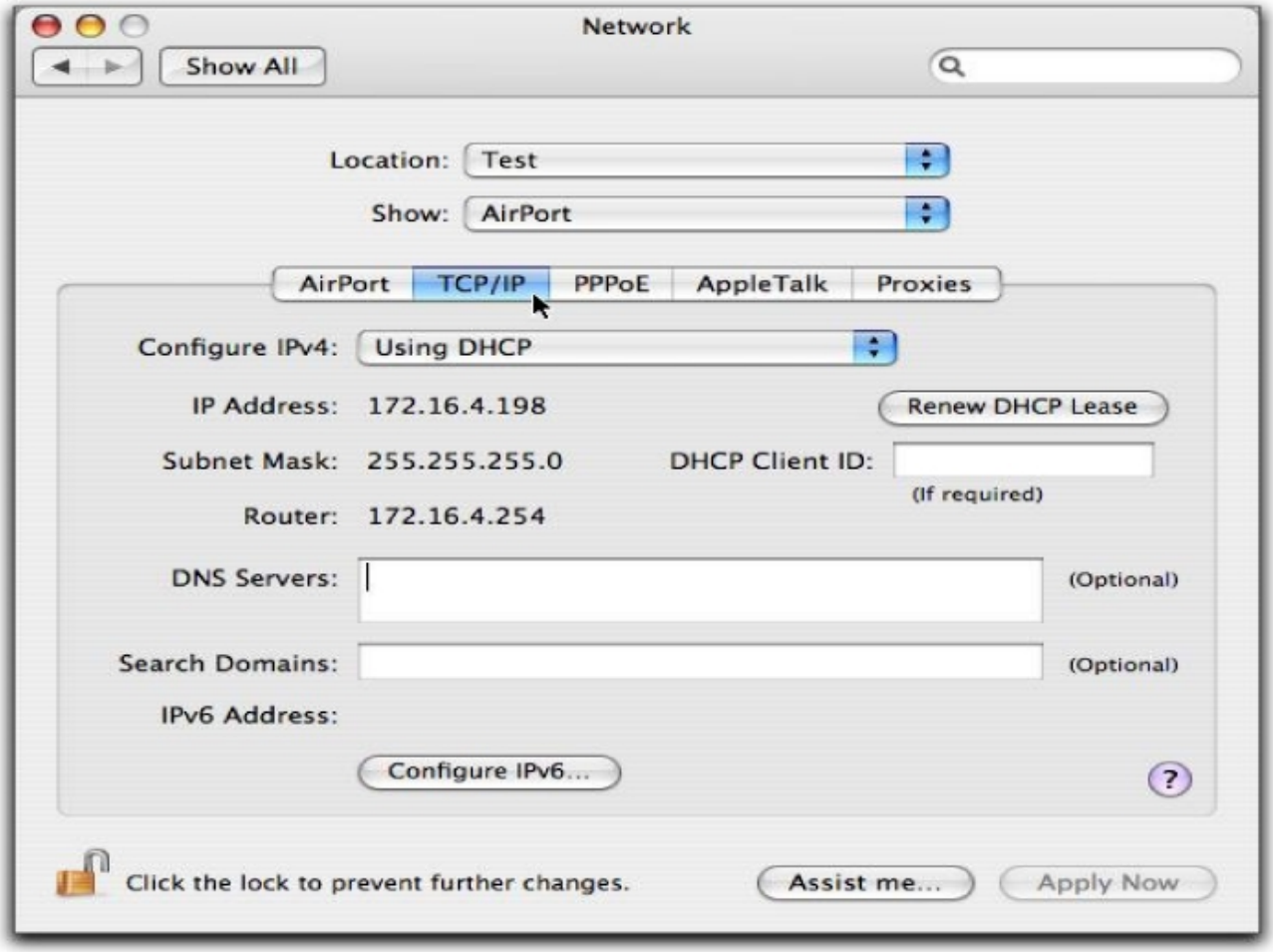
Windows XP

1. Double-click the network icon in the taskbar to display the **Wireless Network Connection Status** window.
   Check that the correct network is listed in the **Connection** section.
2. Select the **Support** tab.
   Check that the **Address Type** is **Assigned by DHCP**. Check that the **IP Address**, **Subnet Mask**, and **Default Gateway** values are valid.
3. Select **Details** to view the DNS server addresses.
   The listed address should be the DNS serves that were assigned to the WAP. Usually a wireless network that provides access to the private LAN is assigned the same DNS servers as the wired private LAN. A wireless network that provides guest or customer users access to the Internet is usually assigned public DNS servers.
4. If any of the addresses are missing, select **Repair**.
   If the repair procedure doesn't correct the problem, check your network settings.

Mac OS

1. From the Apple menu, open **System Preferences > Network**.
2. Select **AirPort** and then select **Configure**.

3. On the **Network** page, select the **TCP/IP** tab.



4. If there is no IP address or the IP address starts with 169, select **Renew DHCP Lease**.
5. To check DNS server addresses, open a terminal window and enter the following command:

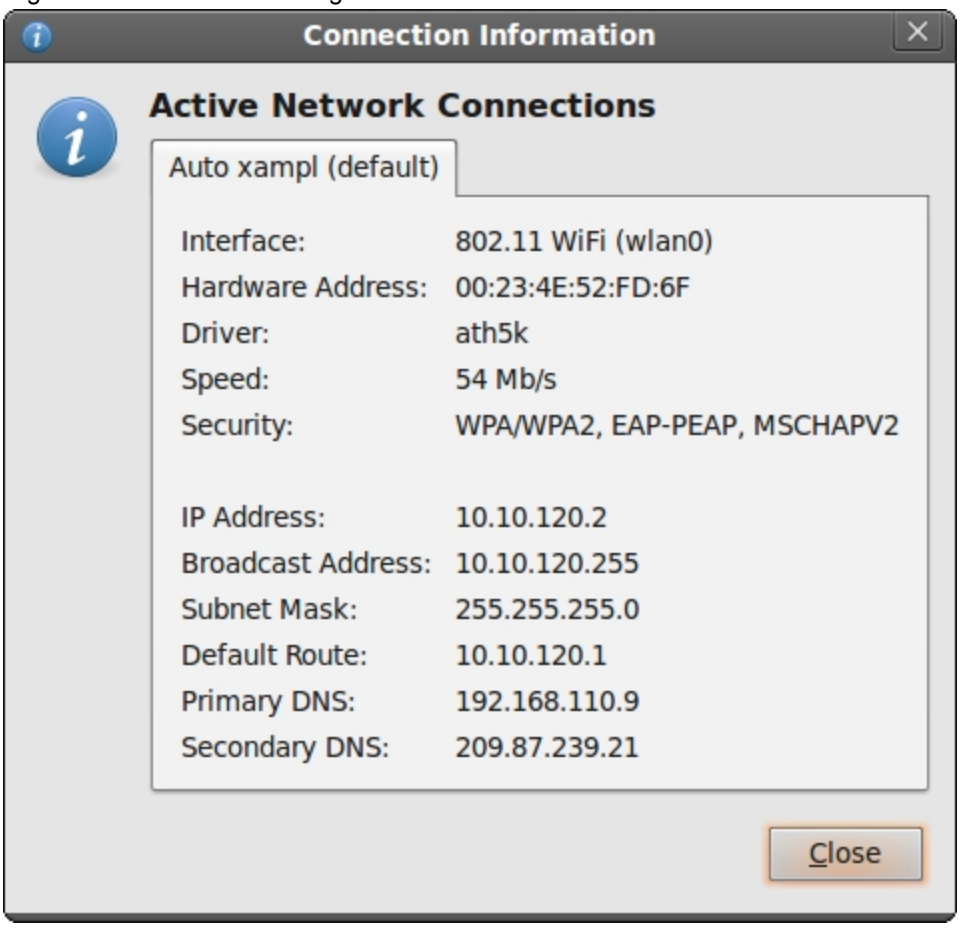
   ```
   cat /etc/resolv.conf
   ```

   Check the listed nameserver addresses. A network for employees should us the wired private LAN DNS server. A network for guests should specify a public DNS server.

Linux

This example is based on the Ubuntu 10.04 Linux wireless client.

1. Right-click the Network Manager icon and select **Connection Information**.



2. Check the IP address, and DNS settings. If they are incorrect, check your network settings.

Wireless network examples

This chapter provides an example wireless network configuration.

Basic wireless network
A more complex example

Basic wireless network

This example uses automatic configuration to set up a basic wireless network.

To configure this wireless network, you must:

- Configure authentication for wireless users
- Configure the SSID (WiFi network interface)
- Add the SSID to the FortiAP Profile
- Configure the firewall policy
- Configure and connect FortiAP units

Configuring authentication for wireless users

You need to configure user accounts and add the users to a user group. This example shows only one account, but multiple accounts can be added as user group members.

To configure a WiFi user - web-based manager

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next.**
5. Make sure that **Enable** is selected and then click **Create**.

To configure the WiFi user group - web-based manager

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	wlan_users
Type	**Firewall**
Members	Add users.

To configure a WiFi user and the WiFi user group - CLI

```
config user user
   edit "user01"
      set type password
      set passwd "asdf12ghjk"
```

```
    end
  config user group
    edit "wlan_users"
      set member "user01"
    end
```

Configuring the SSID

First, establish the SSID (network interface) for the network. This is independent of the number of physical access points that will be deployed. The network assigns IP addresses using DHCP.

To configure the SSID - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Enter the following information and select **OK**:

Interface Name		example_wifi_if
Traffic Mode		Tunnel to Wireless Controller
IP/Network Mask		10.10.110.1/24
Administrative Access		Ping (to assist with testing)
DHCP Server		Enable
	Address Range	10.10.110.2 - 10.10.110.199
	Netmask	255.255.255.0
	Default Gateway	Same As Interface IP
	DNS Server	Same as System DNS
SSID		example_wifi
Security Mode		WPA2 Enterprise
Authentication		Usergroup, select **wlan_users**.
Leave other settings at their default values.		

To configure the SSID - CLI

```
config wireless-controller vap
  edit example_wifi_if
    set ssid "example_wifi"
    set broadcast-ssid enable
    set security wpa-enterprise
    set auth usergroup
    set usergroup wlan_users
  end
config system interface
  edit example_wifi_if
    set ip 10.10.110.1 255.255.255.0
  end
```

```
config system dhcp server
   edit 0
        set default-gateway 10.10.110.1
      set dns-service default
      set interface "example_wifi_if"
      config ip-range
         edit 1
            set end-ip 10.10.110.199
            set start-ip 10.10.110.2
         end
      set netmask 255.255.255.0
   end
```

Adding the SSID to the FortiAP Profile

The radio portion of the FortiAP configuration is contained in the FortiAP Profile. By default, there is a profile for each platform (FortiAP model). You can create additional profiles if needed. The SSID needs to be specified in the profile.

To add the SSID to the FortiAP Profile - web-based manager

1. Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile for your model of FortiAP unit.
2. In **Radio 1** and **Radio 2**, add example_wifi in **SSID**.
3. Select **OK**.

Configuring firewall policies

A firewall policy is needed to enable WiFi users to access the Internet on port1. First you create firewall address for the WiFi network, then you create the example_wifi to port1 policy.

To create a firewall address for WiFi users - web-based manager

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

Name	wlan_user_net
Type	Subnet
Subnet / IP Range	10.10.110.0/24
Interface	example_wifi_if
Visibility	Enabled

To create a firewall address for WiFi users - CLI

```
config firewall address
   edit "wlan_user_net"
      set associated-interface "example_wifi_if"
      set subnet 10.10.110.0 255.255.255.0
   end
```

To create a firewall policy for WiFi users - web-based manager

1. Go to **Policy & Objects > Policy > IPv4**and select **Create New**.
2. Enter the following information and select **OK**:

Incoming Interface	example_wifi_if
Source Address	wlan_user_net
Outgoing Interface	port1
Destination Address	All
Schedule	always
Service	ALL
Action	ACCEPT
NAT	ON. Select **Use Destination Interface Address** (default).
Leave other settings at their default values.	

To create a firewall policy for WiFi users - CLI

```
config firewall policy
   edit 0
      set srcintf "example_wifi"
      set dstintf "port1"
      set srcaddr "wlan_user_net"
      set dstaddr "all"
      set schedule always
      set service ALL
      set action accept
      set nat enable
   end
```

Connecting the FortiAP units

You need to connect each FortiAP unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

To configure the interface for the AP unit - web-based manager

1. Go to **System > Network > Interfaces** and edit the port3 interface.
2. Set the **Addressing mode** to **Dedicate to Extension Device** and set the **IP/Network Mask** to `192.168.8.1/255.255.255.0`.
3. Select **OK**.

This procedure automatically configures a DHCP server for the AP units. You can see this configuration in **System > Network > DHCP Server**.

To configure the interface for the AP unit - CLI

```
config system interface
   edit port3
      set mode static
      set ip 192.168.8.1 255.255.255.0
   end
```

To configure the DHCP server for AP units - CLI

```
config system dhcp server
   edit 0
      set interface port3
      config exclude-range
         edit 1
            set end-ip 192.168.8.1
            set start-ip 192.168.8.1
         end
      config ip-range
         edit 1
            set end-ip 192.168.8.254
            set start-ip 192.168.8.2
         end
         set netmask 255.255.255.0
         set vci-match enable
         set vci-string "FortiAP"
   end
```

To connect a FortiAP unit - web-based manager

1. Go to **WiFi Controller > Managed Devices > Managed FortiAPs**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If FortiAP units are connected but cannot be recognized, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize.**
6. In **FortiAP Profile**, select the default profile for the FortiAP model.
   Override Settings should **not** be selected.
7. Select **OK**.
8. Repeat Steps 2 through 8 for each FortiAP unit.

To connect a FortiAP unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter
   ```
   config wireless-controller wtp
   ```

3. Wait 30 seconds, then enter `get`.
   Retry the `get` command every 15 seconds or so until the unit is listed, like this:
   ```
   == [ FAP22B3U10600118 ]
   wtp-id: FAP22B3U10600118
   ```

4. Edit the discovered FortiAP unit like this:
   ```
   edit FAP22B3U10600118
      set admin enable
   end
   ```

5. Repeat Steps 2 through 4 for each FortiAP unit.

A more complex example

This example creates multiple networks and uses custom AP profiles.

Scenario

In this example, Example Co. provides two wireless networks, one for its employees and the other for customers or other guests of its business. Guest users have access only to the Internet, not to the company's private network. The equipment for these WiFi networks consists of FortiAP-220B units controlled by a FortiGate unit.

The employee network operates in 802.11n mode on both the 2.4GHz and 5GHz bands. Client IP addresses are in the 10.10.120.0/24 subnet, with 10.10.120.1 the IP address of the WAP. The guest network also operates in 802.11n mode, but only on the 2.4GHz band. Client IP addresses are on the 10.10.115.0/24 subnet, with 10.10.115.1 the IP address of the WAP.

On FortiAP-220B units, the 802.11n mode also supports 802.11g and 802.11b clients on the 2.4GHz band and 802.11a clients on the 5GHz band.

The guest network WAP broadcasts its SSID, the employee network WAP does not.

The employees network uses WPA-Enterprise authentication through a FortiGate user group. The guest network features a captive portal. When a guest first tries to connect to the Internet, a login page requests logon credentials. Guests use numbered guest accounts authenticated by RADIUS. The captive portal for the guests includes a disclaimer page.

In this example, the FortiAP units connect to port 3 and are assigned addresses on the 192.168.8.0/24 subnet.

Configuration

To configure these wireless networks, you must:

- Configure authentication for wireless users
- Configure the SSIDs (network interfaces)
- Configure the AP profile
- Configure the WiFi LAN interface and a DHCP server
- Configure firewall policies

Configuring authentication for employee wireless users

Employees have user accounts on the FortiGate unit. This example shows creation of one user account, but you can create multiple accounts and add them as members to the user group.

To configure a WiFi user - web-based manager

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next**.
5. Make sure that **Enable** is selected and then click **Create**.

To configure the user group for employee access - web-based manager

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	employee-group
Type	**Firewall**
Members	Add users.

To configure a WiFi user and the user group for employee access - CLI

```
config user user
   edit "user01"
      set type password
      set passwd "asdf12ghjk"
   end
config user group
   edit "employee-group"
      set member "user01"
   end
```

The user authentication setup will be complete when you select the employee-group in the SSID configuration.

Configuring authentication for guest wireless users

Guests are assigned temporary user accounts created on a RADIUS server. The RADIUS server stores each user's group name in the Fortinet-Group-Name attribute. Wireless users are in the group named "wireless".

The FortiGate unit must be configured to access the RADIUS server.

To configure the FortiGate unit to access the guest RADIUS server - web-based manager

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information and select OK:

Name	guestRADIUS
Primary Server IP/Name	10.11.102.100
Primary Server Secret	grikfwpfdfg
Secondary Server IP/Name	Optional

Secondary Server Secret	Optional
Authentication Scheme	Use default, unless server requires otherwise.
Leave other settings at their default values.	

To configure the FortiGate unit to access the guest RADIUS server - CLI

```
config user radius
   edit guestRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret grikfwpfdfg
   end
```

To configure the user group for guest access - web-based manager

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	guest-group
Type	**Firewall**
Members	Leave empty.

3. Select **Add**.
4. Enter:

Remote Server	Select **guestRADIUS**.
Group Name	Select **Specify** and then enter `wireless`

5. Select **OK**.

To configure the user group for guest access - CLI

```
config user group
   edit "guest-group"
      set member "guestRADIUS"
      config match
         edit 0
            set server-name "guestRADIUS"
            set group-name "wireless"
         end
   end
```

The user authentication setup will be complete when you select the guest-group user group in the SSID configuration.

Configuring the SSIDs

First, establish the SSIDs (network interfaces) for the employee and guest networks. This is independent of the number of physical access points that will be deployed. Both networks assign IP addresses using DHCP.

To configure the employee SSID - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Enter the following information and select **OK**:

Interface Name	example_inc
IP/Netmask	10.10.120.1/24
Traffic Mode	Tunnel to Wireless Controller
Administrative Access	Ping (to assist with testing)
SSID	example_inc
Enable DHCP	Enable
Address Range	10.10.120.2 - 10.10.120.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
DNS Server	Same as System DNS
Security Mode	WPA/WPA2-Enterprise
Authentication	Select **Usergroup**, then select **employee-group.**
Leave other settings at their default values.	

To configure the employee SSID - CLI

```
config wireless-controller vap
   edit example_inc
      set ssid "example_inc"
      set security wpa-enterprise
      set auth usergroup
      set usergroup employee-group
   end
config system interface
   edit example_inc
      set ip 10.10.120.1 255.255.255.0
   end
config system dhcp server
   edit 0
      set default-gateway 10.10.120.1
      set dns-service default
      set interface example_inc
      config ip-range
         edit 1
```

```
            set end-ip 10.10.120.199
            set start-ip 10.10.120.2
         end
      set lease-time 7200
      set netmask 255.255.255.0
   end
```

To configure the example_guest SSID - web-based manager

1. Go to **WiFi Controller > WiFi Network > SSID** and select **Create New**.
2. Enter the following information and select **OK**:

Name	example_guest
IP/Netmask	10.10.115.1/24
Administrative Access	Ping (to assist with testing)
SSID	example_guest
Enable DHCP	Enable
Address Range	10.10.115.2 - 10.10.115.50
Netmask	255.255.255.0
Default Gateway	Same as Interface IP
DNS Server	Same as System DNS
Security Mode	Captive Portal
Customize Portal Messages	Select
User Groups	Select **guest-group**
Leave other settings at their default values.	

To configure the example_guest SSID - CLI

```
config wireless-controller vap
   edit example_guest
      set ssid "example_guest"
      set security captive-portal
      set selected-usergroups guest-group
   end
config system interface
   edit example_guest
      set ip 10.10.115.1 255.255.255.0
   end
config system dhcp server
   edit 0
      set default-gateway 10.10.115.1
      set dns-service default
      set interface "example_guest"
      config ip-range
         edit 1
```

```
            set end-ip 10.10.115.50
            set start-ip 10.10.115.2
        end
        set lease-time 7200
        set netmask 255.255.255.0
    end
```

Configuring the FortiAP profile

The FortiAP Profile defines the radio settings for the networks. The profile provides access to both Radio 1 (2.4GHz) and Radio 2 (5GHz) for the employee virtual AP, but provides access only to Radio 1 for the guest virtual AP.

To configure the FortiAP Profile - web-based manager

1. Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and select **Create New**.
2. Enter the following information and select **OK**:

Name	example_AP
Platform	FAP220B
Radio 1	
Mode	Access Point
Spectrum Analysis	Enable
Radio Resource Provision	Not enabled
Band	802.11n
Short Guard Interval	Not enabled
Channel	Select 1, 6, and 11.
Tx Power	100%
SSID	Select **example_inc** and **example_guest**.
Radio 2	
Mode	Access Point
Spectrum Analysis	Enable
Radio Resource Provision	Enabled
Band	802.11n_5G
Short Guard Interval	Not enabled
20/40 MHz Channel Width	Not enabled
Channel	Select all.

Tx Power	100%
SSID	Select **example_inc**.

To configure the AP Profile - CLI

```
config wireless-controller wtp-profile
   edit "example_AP"
      config platform
         set type 220B
      end
      config radio-1
         set ap-bgscan enable
         set band 802.11n
         set channel "1" "6" "11"
         set vaps "example_inc" "example_guest"
      end
      config radio-2
         set ap-bgscan enable
         set band 802.11n-5G
         set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
         set vaps "example_inc"
      end
```

Configuring firewall policies

Identity-based firewall policies are needed to enable the WLAN users to access the Internet on Port1. First you create firewall addresses for employee and guest users, then you create the firewall policies.

To create firewall addresses for employee and guest WiFi users

1. Go to **Firewall Objects > Address > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

Address Name	employee-wifi-net
Type	Subnet / IP Range
Subnet / IP Range	10.10.120.0/24
Interface	example_inc

3. Select **Create New**, enter the following information and select **OK**.

Address Name	guest-wifi-net
Type	Subnet / IP Range
Subnet / IP Range	10.10.115.0/24
Interface	example_guest

To create firewall policies for employee WiFi users - web-based manager

1. Go to **Policy > Policy** and select **Create New**.
2. Enter the following information and select **OK**:

Source Interface/Zone	example_inc
Source Address	employee-wifi-net
Destination Interface/Zone	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

3. Optionally, select **UTM** and set up UTM features for wireless users.
4. Select **OK**.
5. Repeat steps 1 through 4 but select Internal as the Destination Interface/Zone to provides access to the ExampleCo private network.

To create firewall policies for employee WiFi users - CLI

```
config firewall policy
   edit 0
      set srcintf "employee_inc"
      set dstintf "port1"
      set srcaddr "employee-wifi-net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
      set schedule "always"
      set service "ANY"
   next
   edit 0
      set srcintf "employee_inc"
      set dstintf "internal"
      set srcaddr "employee-wifi-net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
      set schedule "always"
      set service "ANY"
   end
```

To create a firewall policy for guest WiFi users - web-based manager

1. Go to **Policy > Policy** and select **Create New**.
2. Enter the following information and select **OK**:

Source Interface/Zone	example_guest
Source Address	guest-wifi-net
Destination Interface/Zone	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

3. Optionally, select **UTM** and set up UTM features for wireless users.
4. Select **OK**.

To create a firewall policy for guest WiFi users - CLI

```
config firewall policy
   edit 0
      set srcintf "example_guest"
      set dstintf "port1"
      set srcaddr "guest-wifi-net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
   end
```

Connecting the FortiAP units

You need to connect each FortiAP-220A unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

To configure the interface for the AP unit - web-based manager

1. Go to **System > Network > Interfaces** and edit the port3 interface.
2. Set the **Addressing mode** to **Manual** and set the **IP/Netmask** to `192.168.8.1`.
3. Enable **Connect FortiAP to this interface and** set **Reserve IP addresses for FortiAP** to `192.168.8.2 - 192.168.8.9`.

This step automatically configures a DHCP server for the AP units.

4. Select **OK**.

To configure the interface for the AP unit - CLI

```
config system interface
   edit port3
      set mode static
      set ip 192.168.8.1 255.255.255.0
   end
```

To configure the DHCP server for AP units - CLI

```
config system dhcp server
   edit 0
      set interface port3
      config ip-range
         edit 1
            set end-ip 192.168.8.9
            set start-ip 192.168.8.2
         end
      set netmask 255.255.255.0
      set vci-match enable
      set vci-string "FortiAP"
   end
```

To connect a FortiAP-220A unit - web-based manager

1. Go to **WiFi Controller > Managed Access Points > Managed FortiAP**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If there is persistent difficulty recognizing FortiAP units, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize.**
6. In the **AP Profile,** select **[Change]** and then select the **example_AP** profile.
7. Select **OK**.
8. Repeat Steps 2 through 8 for each FortiAP unit.

To connect a FortiAP-220A unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter:
   ```
   config wireless-controller wtp
   ```
3. Wait 30 seconds, then enter `get`.
   Retry the `get` command every 15 seconds or so until the unit is listed, like this:
   ```
   == [ FAP22A3U10600118 ]
   wtp-id: FAP22A3U10600118
   ```
4. Edit the discovered FortiAP unit like this:

```
edit FAP22A3U10600118
   set admin enable
   set wtp-profile example_AP
end
```

5. Repeat Steps 2 through 4 for each FortiAP unit.

Using a FortiWiFi unit as a client

A FortiWiFi unit by default operates as a wireless access point. But a FortiWiFi unit can also operate as a wireless client, connecting the FortiGate unit to another wireless network.

Use of client mode
Configuring client mode

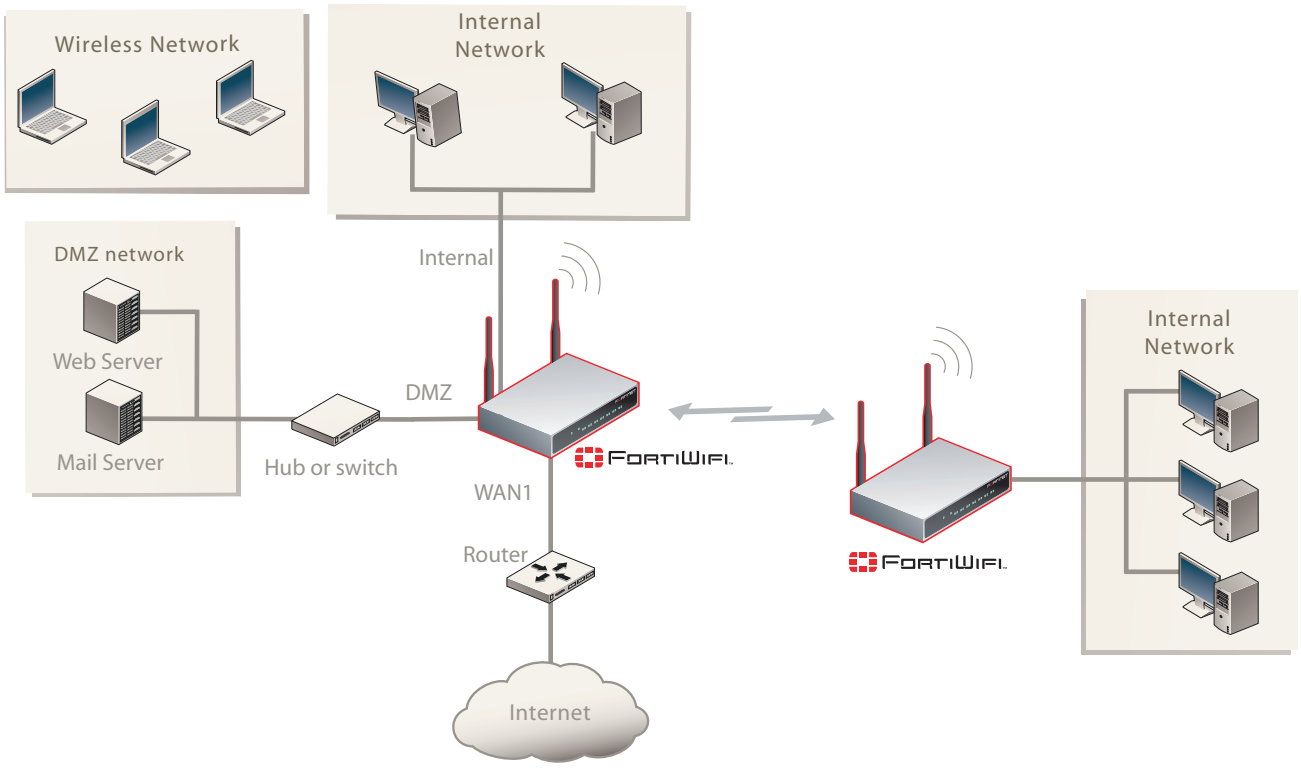
Use of client mode

In client mode, the FortiWiFi unit connects to a remote WiFi access point to access other networks or the Internet. This is most useful when the FortiWiFi unit is in a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables might not be an option due to the warehouse environment. The FortiWiFi unit can support wired users using its Ethernet ports and can connect to another access point wirelessly as a client. This connects the wired users to the network using the 802.11 WiFi standard as a backbone.

Note that in client mode the FortiWiFi unit cannot operate as an AP. WiFi clients cannot see or connect to the FortiWifi unit in Client mode.

Fortinet unit in Client mode



Configuring client mode

To set up the FortiAP unit as a WiFi client, you must use the CLI. Before you do this, be sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and so on.

To configure wireless client mode

1. Change the WiFi mode to client.
   In the CLI, enter the following commands:
   ```
   config system global
      set wireless-mode client
   end
   ```
   Respond “y” when asked if you want to continue. The FortiWiFi unit will reboot.
2. Configure the WiFi interface settings.
   For example, to configure the client for WPA-Personal authentication on the **our_wifi** SSID with passphrase **justforus**, enter the following in the CLI:
   ```
   config system interface
      edit wifi
         set mode dhcp
         config wifi-networks
            edit 0
               set wifi-ssid our_wifi
               set wifi-security wpa-personal
               set wifi-passphrase "justforus"
            end
      end
   ```
   The WiFi interface client_wifi will receive an IP address using DHCP.
3. Configure a wifi to port1 policy.
   You can use either CLI or web-based manager to do this. The important settings are:

Incoming Interface (srcintf)	wifi
Source Address (srcaddr)	all
Outgoing Interface (dstintf)	port1
Destination Address (dstaddr)	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Selected

Support for location-based services

FortiOS supports location-based services by collecting information about WiFi devices near FortiGate-managed access points, even if the devices don't associate with the network.

Overview
Configuring location tracking
Viewing device location data on the FortiGate unit

Overview

WiFi devices broadcast packets as they search for available networks. The FortiGate WiFi controller can collect information about the interval, duration, and signal strength of these packets. The Euclid Analytics service uses this information to track the movements of the device owner. A typical application of this technology is to analyze shopper behavior in a shopping center. Which stores do people walk past? Which window displays do they stop to look at? Which stores do they enter and how long do they spend there? The shoppers are not personally identified, each is known only by the MAC address of their WiFi device.

After enabling location tracking on the FortiGate unit, you can confirm that the feature is working by using a specialized diagnostic command to view the raw tracking data. The Euclid Analytics service obtains the same data in its proprietary format using a JSON inquiry through the FortiGate unit's web-based manager interface.

Configuring location tracking

You can enable location tracking in any FortiAP profile, using the CLI. For each radio, set the `station-locate` field to `enable`. For example:

```
config wireless-controller wtp-profile
   edit "FAP220B-locate"
      set ap-country US
      config platform
         set type 220B
      end
      config radio-1
         set station-locate enable
      end
      config radio-2
         set station-locate enable
      end
   end
```

Viewing device location data on the FortiGate unit

You can use the FortiGate CLI to list located devices. This is mainly useful to confirm that the location data feature is working, You can also reset device location data.

To list located devices

```
diag wireless-controller wlac -c sta-locate
```

To reset device location data

```
diag wireless-controller wlac -c sta-locate-reset
```

Example output

The following output shows data for three WiFi devices.

```
FWF60C3G11004319 # diagnose wireless-controller wlac -c sta-locate
   sta_mac vfid rid base_mac freq_lst frm_cnt frm_fst frm_last intv_sum intv2_sum intv3_
       sum intv_min intv_max signal_sum signal2_sum signal3_sum sig_min sig_max sig_fst
       sig_last ap

   00:0b:6b:22:82:61 0
   FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 257 708 56 651 1836 6441 0 12 -21832
       1855438 -157758796 -88 -81 -84 -88 0

   00:db:df:24:1a:67 0
   FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 42 1666 41 1625 97210 5831613 0 60 -3608
       310072 -26658680 -90 -83 -85 -89 0

   10:68:3f:50:22:29 0
   FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 102 1623 58 1565 94136 5664566 0 60 -8025
       631703 -49751433 -84 -75 -78 -79 0
```

The output for each device appears on two lines. The first line contains only the device MAC address and the VLAN ID. The second line begins with the ID (serial number) of the FortiWiFi or FortiAP unit that detected the device, the AP's MAC address, and then the fields that the Euclid service uses. Because of its length, this line wraps around and displays as multiple lines.

Reference

This chapter provides some reference information pertaining to wireless networks.

FortiAP web-based manager
Wireless radio channels
FortiAP CLI

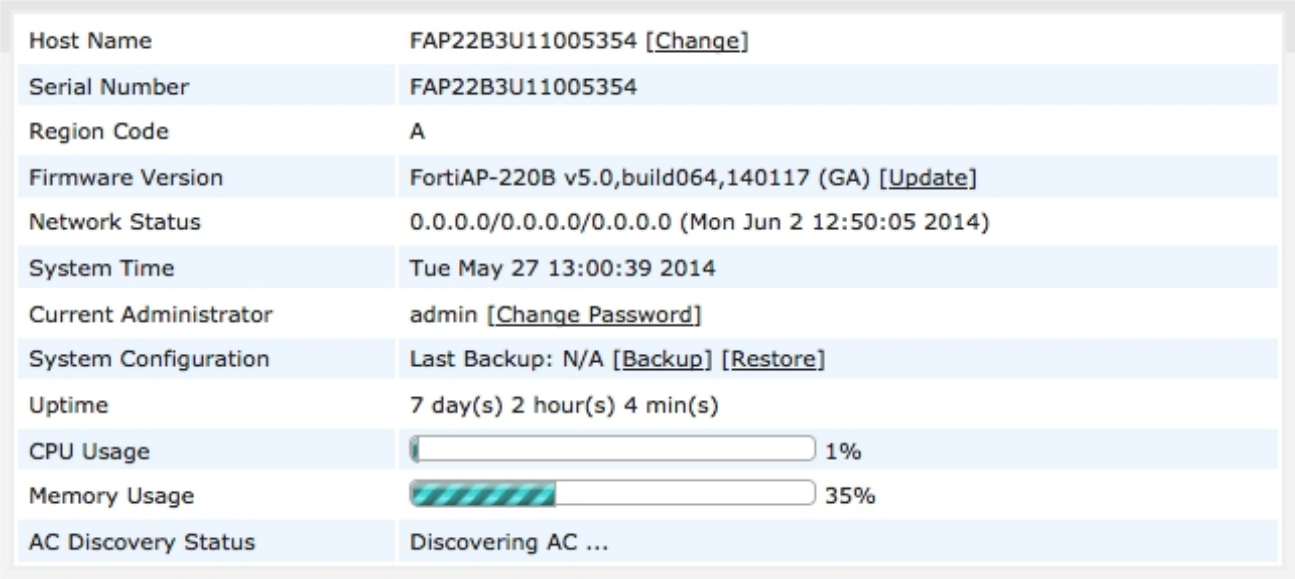
FortiAP web-based manager

You can access the FortiAP unit's built-in web-based manager. This is useful to adjust settings that are not available through the FortiGate unit's WiFi Controller. Logging into the FortiAP web-based manager is similar to logging into the FortiGate web-based manager.

System Information

Status

The **Status** section provides information about the FortiAP unit.



You can:

- Select **Change** to change the **Host Name**.
- Select **Update** in **Firmware Version** to upload a new FortiAP firmware file from your computer.
- Select **Change Password** to change the administrator password.
- Select **Backup** to save the current FortiAP configuration as a file on your computer.
- Select Restore to load a configuration into your FortiAP unit from a file on your computer.

Network Configuration

Select DHCP or select Static and specify the IP address, netmask, and gateway IP address. **Administrative Access** settings affect access after the FortiAP has been authorized. By default, **HTTP** access needed to access the FortiAP web-based manager is enabled, but **Telnet** access is not enabled.

Connectivity

These settings determine how the FortiAP unit connects to the FortiGate WiFi controller.

Uplink	Ethernet - wired connection to the FortiGate unit (default) Mesh - WiFi mesh connection Ethernet with mesh backup support
Mesh AP SSID	Enter the SSID of the mesh root. Default: fortinet.mesh.root
Mesh AP Password	Enter password for the mesh SSID.
Ethernet Bridge	Bridge the mesh SSID to the FortiAP Ethernet port. This is available only whe **Uplink** is **Mesh**.

WTP Configuration

AC Discovery Type settings affect how the FortiAP unit discovers a FortiGate WiFi controller. By default, this is set to Auto which causes the FortiAP unit to cycle through all of the discovery methods until successful. For more information see Controller discovery methods.

AC Discovery Type	Static, DHCP, DNS, Broadcast, Multicast, Auto
AC Control Port	Default port is 5246.
AC IP Address 1 **AC IP Address 2** **AC IP Address 3**	You enter up to three WiFi controller IP addresses for static discovery. Routing must be properly configured in both directions.
AC Host Name 1 **AC Host Name 2** **AC Host Name 3**	As an alternetive to AC IP addresses, you can enter their fully qualified domain names (FQDNs).
AC Discovery Multicast Address	224.0.1.140
AC Discovery DHCP Option Code	When using DHCP discovery, you can configure the DHCP server to provide the controller address. By default the FortiAP unit expects this in option 138.

AC Data Channel Security by default accepts either DTLS-encrypted or clear text data communication with the WiFi controller. You can change this setting to require encryption or to use clear text only.

Wireless Information

The Wireless Information page provides current information about the operation of the radios and the type Uplink in use.

Wireless radio channels

IEEE 802.11a/n channels

The following table lists the channels supported on FortiWiFi products that support the IEEE 802.11a and 802.11n wireless standards. 802.11a is available on FortiWiFi models 60B and higher. 802.11n is available on FortiWiFi models 80CM and higher.

All channels are restricted to indoor usage except in the Americas, where both indoor and outdoor use is permitted on channels 52 through 64 in the United States.

IEEE 802.11a/n (5-GHz Band) channel numbers

Channel number	Frequency (MHz)	Regulatory Areas				
		Americas	Europe	Taiwan	Singapore	Japan
34	5170					•
36	5180	•	•		•	
38	5190					
40	5200	•	•		•	•
42	5210					
44	5220	•	•		•	•
46	5230					
48	5240	•	•		•	•
149	5745	•		•	•	
153	5765	•		•	•	
157	5785	•		•	•	
161	5805	•		•	•	
165	5825	•			•	

IEEE 802.11b/g/n channel numbers

The following table lists IEEE 802.11b/g/n channels. All FortiWiFi units support 802.11b and 802.11g. Newer models also support 802.11n.

Mexico is included in the Americas regulatory domain. Channels 1 through 8 are for indoor use only. Channels 9 through 11 can be used indoors and outdoors. You must make sure that the channel number complies with the regulatory standards of Mexico.

IEEE 802.11b/g/n (2.4-GHz Band) channel numbers

Channel number	Frequency (MHz)	Regulatory Areas			
		Americas	EMEA	Israel	Japan
1	2412	•	•	indoor	•
2	2417	•	•	indoor	•
3	2422	•	•	indoor	•
4	2427	•	•	indoor	•
5	2432	•	•	•	•
6	2437	•	•	•	•
7	2442	•	•	•	•
8	2447	•	•	•	•
9	2452	•	•	•	•
10	2457	•	•	•	•
11	2462	•	•	•	•
12	2467		•	•	•
13	2472		•	•	•
14	2484				b only

FortiAP CLI

The FortiAP CLI controls radio and network operation through the use of variables manipulated with the `cfg` command. There are also diagnostic commands.

The cfg commands include the following:

`cfg -s`	List variables.
`cfg -a var=value`	Add or change a variable value.
`cfg -c`	Commit the change to flash.
`cfg -x`	Reset settings to factory defaults.
`cfg -r var`	Remove variable.
`cfg -e`	Export variables.
`cfg -h`	Display help for all commands.

The configuration variables are:

Var	Description and Values
BAUD_RATE	Console data rate: 9600, 19200, 38400, 57600, or 115200 baud.
WTP_NAME	By default, the name is the FortiAP serial number.
FIRMWARE_UPGRADE	Default is 0.
LOGIN_PASSWD	Administrator login password. By default this is empty.
ADMIN_TIMEOUT	Administrative timeout in minutes. Applies to Telnet and web-based manager sessions. Default is 5 minutes.
ADDR_MODE	How the FortiAP unit obtains its IP address and netmask. DHCP - FortiGate interface assigns address. STATIC - Specify in AP_IPADDR and AP_NETMASK. Default is DHCP.
AP_IPADDR AP_NETMASK IPGW	These variables set the FortiAP unit IP address, netmask and default gateway when ADDR_MODE is STATIC. Default 192.168.1.2 255.255.255.0, gateway 192.168.1.1.
AP_MODE	FortiAP operating mode. 0 - Thin AP (default) 2 - Unmanaged Site Survey mode. See SURVEY variables.
DNS_SERVER	DNS Server for clients. If ADDR_MODE is DHCP the DNS server is automatically assigned.
STP_MODE	Spanning Tree Protocol. 0 is off. 1 is on.
AP_MGMT_VLAN_ID	Non-zero value applies VLAN ID for unit management. Default: 0.
ALLOW_TELNET	0 (Telnet disable), 1 (Telnet enable), 2 (controlled by AC). 2 is default.
ALLOW_HTTP	0 (Http disable), 1 (Http enable), 2 (controlled by AC). 2 is default.

Var	Description and Values
AC_DISCOVERY_TYPE	1 - Static. Specify WiFi Controllers 2 - DHCP 3 - DNS 5 - Broadcast 6 - Multicast 0 - Cycle through all of the discovery types until successful.
AC_IPADDR_1 AC_IPADDR_2 AC_IPADDR_3	WiFi Controller IP addresses for static discovery.
AC_HOSTNAME_1 AC_HOSTNAME_2 AC_HOSTNAME_3	WiFi Controller host names for static discovery.
AC_DISCOVERY_MC_ADDR	Multicast address for controller discovery. Default 224.0.1.140.
AC_DISCOVERY_DHCP_OPTION_CODE	
	Option code for DHCP server. 138 (default)
AC_CTL_PORT	WiFi Controller control (CAPWAP) port. Default 5246.
AC_DATA_CHAN_SEC	Data channel security. 0 - Clear text 1 - DTLS (encrypted) 2 - Accept either DTLS or clear text (default)
MESH_AP_TYPE	Type of communication for backhaul to controller: 0 - Ethernet (default) 1 - WiFi mesh 2 - Ethernet with mesh backup support
MESH_AP_SSID	SSID for mesh backhaul. Default: fortinet.mesh.root

Var	Description and Values
MESH_AP_BSSID	WiFi MAC address
MESH_AP_PASSWD	Pre-shared key for mesh backhaul.
MESH_ETH_BRIDGE	1 - Bridge mesh WiFi SSID to FortiAP Ethernet port. This can be used for point-to-point bridge configuration. This is available only when MESH_AP_TYPE =1. 0 - No WiFi-Ethernet bridge (default).
MESH_MAX_HOPS	Maximum number of times packets can be passed from node to node on the mesh. Default is 4.
The following factors are summed and the FortiAP associates with the lowest scoring mesh AP.	
MESH_SCORE_HOP_WEIGHT	Multiplier for number of mesh hops from root. Default 50.
MESH_SCORE_CHAN_WEIGHT	AP total RSSI multiplier. Default 1.
MESH_SCORE_RATE_WEIGHT	Beacon data rate multiplier. Default 1.
MESH_SCORE_BAND_WEIGHT	Band weight (0 for 2.4GHz, 1 for 5GHz) multiplier. Default 100.
MESH_SCORE_RSSI_WEIGHT	AP channel RSSI multiplier. Default 100.
SURVEY_SSID	SSID to broadcast in site survey mode (AP_MODE=2).
SURVEY_TX_POWER	Transmitter power in site survey mode (AP_MODE=2).
SURVEY_CH_24	Site survey transmit channel for the 2.4Ghz band (default 6).
SURVEY_CH_50	Site survey transmit channel for the 5Ghz band (default 36).
SURVEY_BEACON_INTV	Site survey beacon interval. Default 100msec.
WTP_LOCATION	Optional string describing AP location.

Diagnose commands include:

`cw_diag help`	Display help for all diagnose commands.
`cw_diag uptime`	Show daemon uptime.
`cw_diag --tlog <on|off>`	Turn on/off telnet log message.
`cw_diag --clog <on|off>`	Turn on/off console log message.
`cw_diag baudrate [9600 | 19200 | 38400 | 57600 | 115200]`	Set the console baud rate.
`cw_diag plain-ctl [0|1]`	Show or change current plain control setting.
`cw_diag sniff-cfg ip port`	Set sniff server ip and port.
`cw_diag sniff [0|1|2]`	Enable/disable sniff packet.
`cw_diag stats wl_intf`	Show wl_intf status.
`cw_diag admin-timeout [30]`	Set shell idle timeout in minutes.
`cw_diag -c wtp-cfg`	Show current wtp config parameters in control plane.
`cw_diag -c radio-cfg`	Show current radio config parameters in control plane.
`cw_diag -c vap-cfg`	Show current vaps in control plane.
`cw_diag -c ap-rogue`	Show rogue APs pushed by AC for on-wire scan.
`cw_diag -c sta-rogue`	Show rogue STAs pushed by AC for on-wire scan.
`cw_diag -c arp-req`	Show scanned arp requests.
`cw_diag -c ap-scan`	Show scanned APs.
`cw_diag -c sta-scan`	Show scanned STAs.
`cw_diag -c sta-cap`	Show scanned STA capabilities.
`cw_diag -c wids`	Show scanned WIDS detections.
`cw_diag -c darrp`	Show darrp radio channel.
`cw_diag -c mesh`	Show mesh status.
`cw_diag -c mesh-veth-acinfo`	Show mesh veth ac info, and mesh ether type.
`cw_diag -c mesh-veth-vap`	Show mesh veth vap.

`cw_diag -c mesh-veth-host`	Show mesh veth host.
`cw_diag -c mesh-ap`	Show mesh ap candidates.
`cw_diag -c scan-clr-all`	Flush all scanned AP/STA/ARPs.
`cw_diag -c ap-suppress`	Show suppressed APs.
`cw_diag -c sta-deauth`	De-authenticate an STA.

Chapter 9 - Firewall

"Firewall concepts" explains the ideas behind the components, techniques and processes that are involved in setting up and running a firewall in general, and the FortiGate firewall in particular. Regardless of how experienced someone is with firewalls, as they go through the process of configuring a firewall new to them they are likely to come across a term or setting that they may not be familiar with. FortiGate firewalls are quite comprehensive and can be very granular in the functions they perform, so it makes sense to have a consistent frame of reference for the ideas we will be working with.

Some examples of the concepts that will be addressed here are:

- "What is a Firewall?"
- "NAT"
- "IPv6"

"Firewall objects" describes the following:

- Addressing
- Services
- Firewall Policies

"Network defense" describes various methods of defending your network using the abilities of the FortiGate firewall.

"GUI and CLI - what you may not know" helps you navigate and find the components in the Web-based Manager that you will need to build the functions. This section does not include any in-depth explanations of what each object does as that is covered in the concepts section. This section is for showing you where you need to input your information and letting you know what format the interface expects to get that information

"Building firewall objects and policies" is similar to a cookbook in that it will refer to a number of common tasks that you will likely perform to get the full functionality out of your FortiGate firewall. Because of the way that firewalls are designed, performing many of the tasks requires that firewall components be set up in a number of different sections of the interface and be configured to work together to achieve the desired result. This section will bring those components together as a straight forward series of instructions.

"Multicast forwarding" is a reference guide including the concepts and examples that are involved in the use of multicast addressing and policy forwarding as it is used in the FortiGate firewall.

FortiGate Firewall Components

The FortiGate firewall is made up of a number of different components that are used to build an impressive list of features. These features have flexibility of scope and granularity of control that provide protection far beyond that provided by the basic firewalls of the past.

Some of the components that FortiOS uses to build features are:

- Interfaces
- VLANs
- Soft switches

- Zones
- Predefined addresses
  - IP address-based
  - FQDN-based
  - Geography-based
- Access schedules
- Authentication
  - Local user-based
  - Authentication server-based (Active Directory, RADIUS, LDAP)
  - Device-based
- Configurable services
- IPv4 and IPv6 protocol support

The features of FortiOS include but are not limited to:

- Security profiles, sometimes referred to as Unified Threat Management (UTM) or Next Generation Firewall (NGFW)
- Predefined firewall addresses (this includes IPv4 and IPv6, IP pools, wildcard addresses and netmasks, and geography-based addresses)
- Monitoring traffic
- Traffic shaping and per-IP traffic shaping (advanced)
- Firewall schedules
- Services (such as AOL, DHCP and FTP)
- Logging traffic
- Quality of Service (QoS)
- Identity-based policies
- Endpoint security

The "Firewall concepts" expand on what each of the features does and how they relate to the administration of the FortiGate firewall. The section will also try to explain some of the common firewall concepts that will be touched on in the implementing of these features.

"Building firewall objects and policies" shows how to perform specific tasks with the FortiGate firewall.

How does a FortiGate protect your network?

The FortiGate firewall protects your network by taking the various components and using them together to build a kind of wall or access control point so anyone that is not supposed to be on your network is prevented from accessing your network in any way other than those approved by you. It also protects your network from itself by keeping things that shouldn't happen from happening and optimizing the flow of traffic so the network is protected from traffic congestion that would otherwise impede traffic flow.

Most people have at one time or another played with a child's toy system made up of interlocking blocks. The blocks come in different shapes and sizes so you can build structures to suit your needs. The components of the FortiGate firewall are similar. You are not forced to use all of the blocks all of the time. You mix and match them to get the results that you are looking for. You can build a very basic structure, where its only function is to direct traffic in and out to the correct subnets. You can build a fortress that only allows specific traffic to or from specific hosts at specific times of day and only when credentials that have been pre-approved have been provided. You can also add in that all of the traffic is encrypted, so that even when the traffic is out on the Internet it is private

from the world. Just like the interlocking blocks, what you build is up to you, but chances are if you put them together the right way there isn't much that can't be built.

Here is one example of how the components could be put together to support the requirements of a network infrastructure design.

- Off the internal interface you could have separate VLANs. One for each department of Sales, Marketing and Engineering so the traffic from the users on one VLAN does not intrude upon the hosts of the other VLANs and each department is isolated from the others for security reasons.
- To ease in the administration, each of the VLAN sub-interfaces is made a member of a zone so security policies that apply to all hosts on all the VLANs can be applied to all of them at once.
- Using the addresses component, each of the IP address ranges could be assigned a user-friendly name so they could be referred to individually. For policies that would refer to them all as a whole, the individual ranges can be made members of an address group.
- Firewall schedules could be created to address the differing needs of each of the groups so that Sales and Marketing could be allowed access to the Internet during regular business hours and the Engineering department could be allowed access during the lunch break.
- By setting up the outgoing policies to use FortiGuard Web-filtering, the employees could be prevented from visiting inappropriate sites and thus enforcing the policies of the HR department.
- A couple of virtual IP addresses with port forwarding could be configured to allow users on the Internet access to a web server on the DMZ subnet using the company's only Public IP address.This would not affect the traffic that goes to the company's mail server hosted on a completely different computer.
- Even though the Web server on the same DMZ has an FTP service to allow for the uploading of web pages to the web server from the Marketing and Engineer teams, by placing a DENY policy on any FTP traffic from the Internet, malicious users are prevented from abusing the FTP service.
- By monitoring the traffic as it goes through the policies, you can verify that the policies are in working order.
- By using a combination of ALLOW and DENY policies and placing them in the correct order, you could arrange for an outside contractor to be allowed to update the web site as well.

This list of possible configurations is not extensive, but it does give an idea of how different components can be mixed and matched to build a configuration that meets an organization's needs and at the same time protect it from security risks.

Firewall concepts

There are a number of concepts that are consistent throughout the firewall industry. Having a solid grasp of these ideas and terms can give you a better idea of what your FortiGate firewall is capable of and how it will fit within your network's architecture.

This chapter describes the following firewall concepts:

- What is a Firewall?
- IPv6
- NAT
- How packets are handled by FortiOS
- FortiGate modes
- Quality of Service
- Interfaces and zones

What is a firewall?

The term firewall originally referred to a wall intended to confine a fire or potential fire within a building. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment.

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network such as the Internet, that is not assumed to be secure and trusted.

Network layer or packet filter firewalls

Stateless firewalls

Stateless firewalls are the oldest form of these firewalls. They are faster and simple in design requiring less memory because they process each packet individually and don't require the resources necessary to hold onto packets like stateful firewalls. Stateful firewalls inspect each packet individually and check to see if it matches a predetermined set of rules. According to the matching rule, the packet is either allowed, dropped or rejected. In the case of a rejection, an error message is sent to the source of the traffic. Each packet is inspected in isolation and information is only gathered from the packet itself. Simply put, if the packets were not specifically allowed according to the list of rules held by the firewall, they were not getting through.

Stateful firewalls

Stateful firewalls retain packets in memory so that they can maintain context about active sessions and make judgments about the state of an incoming packet's connection. This enables Stateful firewalls to determine if a packet is the start of a new connection, a part of an existing connection, or not part of any connection. If a packet is part of an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing. If a packet does not match an existing connection, it will be evaluated according to the

rules set for new connections. Predetermined rules are used in the same way as a stateless firewall but they can now work with the additional criteria of the state of the connection to the firewall.

Best Practices Tip for improving performance:

Blocking the packets in a denied session can take more cpu processing resources than passing the traffic through. By putting denied sessions in the session table, they can be kept track of in the same way that allowed session are so that the FortiGate unit does not have to redetermine whether or not to deny all of the packets of a session individually. If the session is denied all packets of that session are also denied.

In order to configure this you will need to use 2 CLI commands

```
config system setting
     set ses-denied-traffic enable
     set block-session-timer <integer 1 - 300>
```
(this determines in seconds, how long, the session is kept in the table)
```
end
```

Application layer firewalls

Application layer filtering is yet another approach and as the name implies it works primarily on the Application Layer of the OSI Model.

Application Layer Firewalls actually, for lack of a better term, understand certain applications and protocols. Examples would be FTP, DNS and HTTP. This form of filtration is able to check to see if the packets are actually behaving incorrectly or if the packets have been incorrectly formatted for the protocol that is indicated. This process also allows for the use of deep packet inspection and the sharing of functionality with Intrusion Prevention Systems (IPS).

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender). Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis.

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Proxy servers

A proxy server is an appliance or application that acts as an intermediary for communicating between computers. A computer has a request for information. The packets are sent to the designated resource but before they can get there they are blocked by the proxy server saying that it will take the request and pass it on. The Proxy Server processes the request and if it is valid it passes onto the designated computer. The designated computer gets the packet and processes the request, sending the answer back to the proxy server. The proxy server sends the information back to the originating computer. It's all a little like a situation with two people who refuse to talk directly with each other using someone else to take messages back and forth.

From a security stand point a Proxy Server can serve a few purposes:

- Protects the anonymity of the originating computer
- The two computers never deal directly with each other
- Packets that are not configured to be forwarded are dropped before reaching the destination computer.
- If malicious code is sent it will affect the Proxy server with out affecting the originating or sending computer.

Proxies can perform a number of roles including:

- Content Filtering
- Caching
- DNS proxy
- Bypassing Filters and Censorship
- Logging and eavesdropping
- Gateways to private networks
- Accessing service anonymously

Security profiles

Unified Threat Management and Next Generation Firewall are terms originally coined by market research firms and refer to the concept of a comprehensive security solution provided in a single package. It is basically combining of what used to be accomplished by a number of different security technologies all under a single umbrella or in this case, a single device. On the FortiGate firewall this is achieved by the use of Security Profiles and optimized hardware.

In effect it is going from a previous style of firewall that included among its features:

- Gateway Network Firewall
- Routing
- VPN

To a more complete system that includes:

- Gateway Network Firewall
- Routing
- VPN
- Traffic Optimization
- Proxy Services
- Content Filtering
- Application Control
- Intrusion Protection
- Denial of Service Attack Protection
- Anti-virus
- Anti-spam
- Data Leak Prevention
- Endpoint Control of Security Applications
- Load Balancing
- WiFi Access Management
- Authentication Integration into Gateway Security

- Logging
- Reporting

Advantages of using security profiles

- Avoidance of multiple installations.
- Hardware requirements are fewer.
- Fewer hardware maintenance requirements.
- Less space required.
- Compatibility - multiple installations of products increase the probability of incompatibility between systems.
- Easier support and management.
- There is only one product to learn therefore a reduced requirement of technical knowledge.
- Only a single vendor so there are fewer support contracts and Service Level Agreements.
- Easier to incorporated into existing security architecture.
- Plug and play architecture.
- Web based GUI for administration.

IPv6

Internet Protocol version 6 (IPv6) will succeed IPv4 as the standard networking protocol of the Internet. IPv6 provides a number of advances over IPv4 but the primary reason for its replacing IPv4 is its limitation in addresses. IPv4 uses 32 bit addresses which means there is a theoretical limit of 2 to the power of 32. The IPv6 address scheme is based on a 128 bit address or a theoretical limit of 2 to the power of 128.

Possible Addresses:

- IPv4 = 4,294,967,296 (over 4 billion)
- IPv6 = 340,282,366,920,938,463,463,374,607,431,768,211,456 (over 340 undecillion - We had to look that term up. We didn't know what a number followed by 36 digits was either)

Assuming a world population of approximately 8 billion people, IPv6 would allow for each individual to have approximately 42,535,295,865,117,200,000,000,000,000 devices with an IP address. That's 42 quintillion devices.

There is little likelihood that you will ever need to worry about these numbers as any kind of serious limitation in addressing but they do give an idea of the scope of the difference in the available addressing.

Aside from the difference of possible addresses there is also the different formatting of the addresses that will need to be addressed.

A computer would view an IPv4 address as a 32 bit string of binary digits made up of 1s and 0s, broken up into 4 octets of 8 digits separated by a period "."

Example:

10101100.00010000.11111110.00000001

To make number more user friendly for humans we translate this into decimal, again 4 octets separated by a period "."which works out to:

172.16.254.1

A computer would view an IPv6 address as a 128 bit string of binary digits made up of 1s and 0s, broken up into 8 octets of 16 digits separated by a colon ":"

1000000000000001:0000110110111000:1010110000010000:1111111000000001:0000000000000000:0000000000000000:0000000000000000:0000000000000000

To make number a little more user friendly for humans we translate this into hexadecimal, again 8 octets separated by a colon ":" which works out to:

8001:0DB8:AC10:FE01:0000:0000:0000:0000:

Because any four-digit group of zeros within an IPv6 address may be reduced to a single zero or altogether omitted, this address can be shortened further to:

8001:0DB8:AC10:FE01:0:0:0:0

or

8001:0DB8:AC10:FE01::

Some of the other benefits of IPv6 include:

- More efficient routing
- Reduced management requirement
- Stateless auto-reconfiguration of hosts
- Improved methods to change Internet Service Providers
- Better mobility support
- Multi-homing
- Security
- Scoped address: link-local, site-local and global address space

The origins of NAT

In order to understand NAT it helps to know why it was created. At one time, every computer that was part of a network had to have it's own addresses so that the other computers could talk to it. There were a few protocols in use at the time, some of which were only for use on a single network, but of those that were routable, the one that had become the standard for the Internet was IP (Internet Protocol) version 4.

When IP version 4 addressing was created nobody had any idea how many addresses would be needed. The total address range was based on the concept of 2 to the 32nd power, which works out to be 4 294 967 296 potential addresses. Once you eliminate some of those for reserved addresses, broadcast addresses, network addresses, multicasting, etc., you end up with a workable scope of about 3.2 million addressees. This was thought to be more than enough at the time. The designers were not expecting the explosion of personal computing, the World Wide Web or smart phones. As of the beginning of 2012, some estimate the number of computers in the world in the neighborhood of 1 billion, and most of those computer users are going to want to be on the Internet or Search the World Wide Web. In short, we ran out of addresses.

This problem of an address shortage was realized before we actually ran out, and in the mid 1990s 2 technical papers called RFCs numbered 1631 (http://www.ietf.org/rfc/rfc1631.txt) and 1918 (http://tools.ietf.org/html/rfc1918), proposed components of a method that would be used as a solution until a new addressing methodology could be implemented across the Internet infrastructure. For more information on this you can look up IP version 6.

RFC 1631 described a process that would allow networking devices to translate a single public address to multiple private IP addresses and RFC 1918 laid out the use of the private addresses. The addresses that were

on the Internet (Public IP addresses) could not be duplicated for them to work as unique addresses, but behind a firewall, which most large institutions had, they could use their own Private IP addresses for internal use and the internal computers could share the external or Public IP address.

To give an idea on a small scale how this works, image that a company has a need for 200 computer addresses. Before Private IP addresses and NAT the company would have purchased a full Class C address range which would have been 254 usable IP addresses; wasting about 50 addresses. Now with NAT, that company only needs 1 IP address for its 200 computers and this leaves the rest of the IP addresses in that range available for other companies to do the same thing.

NAT gives better value than it would first appear because it is not 253 companies that can use 254 addresses but each of those 254 companies could set up their networking infrastructures to use up to thousands of Private IP addresses, more if they don't all have to talk to the Internet at the same time. This process enabled the Internet to keep growing even though we technically have many more computers networked than we have addresses.

Static NAT

In Static NAT one internal IP address is always mapped to the same public IP address.

In FortiGate firewall configurations this is most commonly done with the use of Virtual IP addressing.

An example would be if you had a small range of IP addresses assigned to you by your ISP and you wished to use one of those IP address exclusively for a particular server such as an email server.

Say the internal address of the Email server was 192.168.12.25 and the Public IP address from your assigned addresses range from 256.16.32.65 to 256.16.32.127. Many readers will notice that because one of the numbers is above 255 that this is not a real Public IP address. The Address that you have assigned to the interface connected to your ISP is 256.16.32.66, with 256.16.32.65 being the remote gateway. You wish to use the address of 256.16.32.70 exclusively for your email server.

When using a Virtual IP address you set the external IP address of 256.16.32.70 to map to 192.168.12.25. This means that any traffic being sent to the public address of 256.16.32.70 will be directed to the internal computer at the address of 192.168.12.25

When using a Virtual IP address, this will have the added function that when ever traffic goes from 192.168.12.25 to the Internet it will appear to the recipient of that traffic at the other end as coming from 256.16.32.70.

You should note that if you use Virtual IP addressing with the Port Forwarding enabled you do not get this reciprocal effect and must use IP pools to make sure that the outbound traffic uses the specified IP address.

Dynamic NAT

Dynamic NAT maps the private IP addresses to the first available Public Address from a pool of possible Addresses. In the FortiGate firewall this can be done by using IP Pools.

Overloading

This is a form of Dynamic NAT that maps multiple private IP address to a single Public IP address but differentiates them by using a different port assignment. This is probably the most widely used version of NAT. This is also referred to as PAT (Port Address Translation) or Masquerading.

An example would be if you had a single IP address assigned to you by your ISP but had 50 or 60 computers on your local network.

Say the internal address of the interface connected to the ISP was 256.16.32.65 (again an impossible address) with 256.16.32.64 being the remote gateway. If you are using this form of NAT any time one of your computers accesses the Internet it will be seen from the Internet as 256.16.32.65. If you wish to test this go to 2 different computers and verify that they each have a different private IP address then go to a site that tells you your IP address such as www.ipchicken.com. You will see that the site gives the same result of 256.16.32.65, if it existed, as the public address for both computers.

As mentioned before this is sometimes called Port Address Translation because network device uses TCP ports to determine which internal IP address is associated with each session through the network device. For example, if you have a network with internal addresses ranging from 192.168.1.1 to 192.168.1.255 and you have 5 computers all trying to connect to a web site which is normally listening on port 80 all of them will appear to the remote web site to have the IP address of 256.16.32.65 but they will each have a different sending TCP port, with the port numbers being somewhere between 1 and 65 535, although the port numbers between 1 to 1024 are usually reserved or already in use. So it could be something like the following:

```
192.168.1.10    256.16.32.65:   port 486
192.168.1.23    256.16.32.65:   port 2409
192.168.1.56    256.16.32.65:   port 53763
192.168.1.109   256.16.32.65:   port 5548
192.168.1.201   256.16.32.65:   port 4396
```

And the remote web server would send the responding traffic back based on those port numbers so the network device would be able to sort through the incoming traffic and pass it on to the correct computer.

Overlapping

Because everybody is using the relative same small selection of Private IP addresses it is inevitable that there will be two networks that share the same network range that will need to talk with each other. This happens most often over Virtual Private Networks or when one organization ends up merging with another. This is a case where a private IP address may be translated into a different private IP address so there are no issues with conflict of addresses or confusion in terms of routing.

An example of this would be when you have a Main office that is using an IP range of 172.16.0.1 to 172.20.255.255 connecting through a VPN to a recently acquired branch office that is already running with an IP range of 172.17.1.1 to 172.17.255.255. Both of these ranges are perfectly valid but because the Branch office range is included in the Main Office range any time the system from the Main office try to connect to an address in the Branch Office the routing the system will not send the packet to the default gateway because according to the routing table the address is in its own subnet.

The plan here would be to NAT in both directions so that traffic from neither side of the firewall would be in conflict and they would be able to route the traffic. Everything coming from the Branch Office could be assigned an address in the 192.168.1.1 to 192.168.1.255 range and everything from the Main office going to the Branch Office could be assigned to an address in the 192.168.10.1 to 192.168.10.255 range.

Benefits of NAT

More IP addresses available while conserving public IP addresses

As explained earlier, this was the original intent of the technology and does not need to be gone into further.

Financial savings

Because an organization does not have to purchase IP addresses for every computer in use there is a significant cost savings due to using the process of Network Address Translation.

Security enhancements

One of the side benefits of the process of NAT is an improvement in security. Individual computers are harder to target from the outside and if port forwarding is being used computers on the inside of a firewall are less likely to have unmonitored open ports accessible from the Internet.

Ease of compartmentalization of your network

With a large available pool of IP addresses to use internally a network administrator can arrange things to be compartmentalized in a rational and easily remembered fashion and networks can be broken apart easily to isolate for reasons of network performance and security.

Example

You have a large organization that for security reasons has certain departments that do not share network resources.

You can have the main section of the organization set up as follows;

Network Devices	192.168.1.1 to 192.168.1.25
Internal Servers	192.168.1.26 to 192.168.1.50
Printers	192.168.1.51 to 192.168.1.75
Administration Personnel	192.168.1.76 to 192.168.1.100
Sales People	192.168.1.101 to 192.168.1.200
Marketing	192.168.1.201 to 192.168.1.250

You could then have the following groups broken off into separate subnets:

Accounting	192.168.100.1 to 192.168.100.255
Research and Development	172.16.1.1 to 172.16.255.255
Executive Management	192.168.50.1 to 192.168.50.255
Web sites and Email Servers	10.0.50.1 to 10.0.50.255

These addresses do not have to be assigned right away but can be used as planned ranges.

NAT in transparent mode

Similar to operating in NAT mode, when operating a FortiGate unit in Transparent mode you can add security policies and:

- Enable NAT to translate the source addresses of packets as they pass through the FortiGate unit.
- Add virtual IPs to translate destination addresses of packets as they pass through the FortiGate unit.
- Add IP pools as required for source address translation

A FortiGate unit operating in Transparent mode normally has only one IP address - the management IP. To support NAT in Transparent mode, you can add a second management IP. These two management IPs must be on different subnets. When you add two management IP addresses, all FortiGate unit network interfaces will respond to connections to both of these IP addresses.

Use the following steps to configure NAT in Transparent mode:

1. Add two management IPs
2. Add an IP pool to the WAN1 interface
3. Add an Internal to WAN1 security policy

You can add the security policy from the web-based manager and then use the CLI to enable NAT and add the IP pool.

The usual practice of NATing in transparent mode makes use of two management IP addresses that are on different subnets, but this is not an essential requirement in every case.

If there is a router between the client systems and the FortiGate unit you can use the router's capabilities of tracking sessions to assign NATed addresses from an IP pool to the clients even if the assigned address don't belong to a subnet on your network.

Example

Client computer has an IP address of 1.1.1.33 on the subnet 1.1.1.0/24.

Router "A" sits between the client computer and the FortiGate (in Transparent mode) with the IP address of 1.1.1.1 on the client's side of the router and the IP address of 192.168.1.211 on the FortiGate's side of the router.

Use NAT to assign addresses from an address pool of 9.9.9.1 to 9.9.9.99 to traffic coming from gateway of 192.168.1.211.

To enable the return traffic to get to the original computer, set up a static route than assigns any traffic with a destination of 9.9.9.0/24 to go through the 192.168.1.211 gateway. As long as the session for the outgoing traffic has been maintained, communication between the client computer and the external system on the other side of the FortiGate will work.

.

Central NAT table

The central NAT table enables you to define, and control with more granularity, the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fix port is defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source

address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

IPv6 in FortiOS

From an administrative point of view IPv6 works almost the same as IPv4 in FortiOS. The primary difference is the use IPv6 format for addresses. There is also no need for NAT if the FortiGate firewall is the interface between IPv6 networks. If the subnets attached to the FortiGate firewall are IPv6 and IPv4 NAT can be configured between the 2 different formats. This will involve either configuring a dual stack routing or IPv4 tunneling configuration. The reason for this is simple. NAT was developed primarily for the purpose of extending the number of usable IPv4 addresses. IPv6's addressing allows for enough available addresses so the NAT is no longer necessary.

When configuring IPv6 in FortiOS, you can create a dual stack route or IPv4-IPv6 tunnel. A dual stack routing configuration implements dual IP layers, supporting both IPv4 and IPv6, in both hosts and routers. An IPv4-IPv6 tunnel is essentially similar, creating a tunnel that encapsulates IPv6 packets within IPv4 headers that carry these IPv6 packets over IPv4 tunnels. The FortiGate unit can also be easily integrated into an IPv6 network. Connecting the FortiGate unit to an IPv6 network is exactly the same as connecting it to an IPv4 network, the only difference is that you are using IPv6 addresses.

By default the IPv6 settings are not displayed in the Web-based Manager. It is just a matter of enabling the display of these feature to use them through the web interface. To enable them just go to **System > Admin > Settings** and select **IPv6 Support on GUI**. Once enabled, you will be able to use IPv6 addresses as well as the IPv4 addressing for the following FortiGate firewall features:

- Static routing
- Policy Routing
- Packet and network sniffing
- Dynamic routing (RIPv6, BGP4+, and OSPFv3)
- IPsec VPN
- DNS
- DHCP
- SSL VPN
- Network interface addressing
- Security Profiles protection
- Routing access lists and prefix lists
- NAT/Route and Transparent mode
- NAT 64 and NAT 66
- IPv6 tunnel over IPv4 and IPv4 tunnel over IPv6
- Logging and reporting
- Security policies
- SNMP
- Authentication
- Virtual IPs and groups
- IPv6 over SCTP
- IPv6-specific troubleshooting, such as ping6

Dual stack routing configuration

Dual stack routing implements dual IP layers in hosts and routers, supporting both IPv6 and IPv4. A dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, and even maintain some IPv4 support indefinitely if that is necessary. Devices that are on this type of network, and connect to the Internet, can query Internet DNS servers for both IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can easily connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 addresses. In the FortiOS dual stack architecture it is not just the basic addressing functions that operate in both versions of IP. The other features of the appliance such as Security Profiles and routing can also use both IP stacks.

If an organization with a mixed network uses an Internet service provider that does not support IPv6, they can use an IPv6 tunnel broker to connect to IPv6 addresses that are on the Internet. FortiOS supports IPv6 tunneling over IPv4 networks to tunnel brokers. The tunnel broker extracts the IPv6 packets from the tunnel and routes them to their destinations.

IPv6 tunneling

IPv6 Tunneling is the act of tunneling IPv6 packets from an IPv6 network through an IPv4 network to another IPv6 network. This is different than Network Address Translation (NAT) because once the packet reaches its final destination the true originating address of the sender will still be readable. The IPv6 packets are encapsulated within packets with IPv4 headers, which carry their IPv6 payload through the IPv4 network. This type of configuration is more appropriate for those who have completely transitional over to IPv6, but need an Internet connection, which is still mostly IPv4 addresses.

The key to IPv6 tunneling is the ability of the 2 devices, whether they are a host or a network device, to be dual stack compatible. They have to be able to work with both IPv4 and IPv6 at the same time. In the process the entry node of the tunnel portion of the path will create an encapsulating IPv4 header and transmit the encapsulated packet. The exit node at the end of the tunnel receives the encapsulated packet. The IPv4 header is removed. The IPv6 header is updated and the IPv6 packet is processed.

There are two types of tunnels in IPv6:

Automatic tunnels	Automatic tunnels are configured by using IPv4 address information embedded in an IPv6 address – the IPv6 address of the destination host includes information about which IPv4 address the packet should be tunneled to.
Configured tunnels	Configured tunnels must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified.

Tunnel configurations

There are a few ways in which the tunneling can be performed depending on which segment of the path between the end points of the session the encapsulation takes place.

Network Device to Network Device	Dual stack capable devices connected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the path taken by the IPv6 packets.
Host to Network Device	Dual stack capable hosts can tunnel IPv6 packets to an intermediary IPv6 or IPv4 network device that is reachable through an IPv4 infrastructure. This type of tunnel spans the first segment of the path taken by the IPv6 packets.
Host to Host	Dual stack capable hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire path taken by the IPv6 packets.
Network Device to Host	Dual stack capable network devices can tunnel IPv6 packets to their final destination IPv6 or IPv4 host. This tunnel spans only the last segment of the path taken by the IPv6 packets.

Regardless of whether the tunnel starts at a host or a network device, the node that does the encapsulation needs to maintain soft state information, such as the maximum transmission unit (MTU), about each tunnel in order to process the IPv6 packets.

Tunneling IPv6 through IPsec VPN

A variation on the tunneling IPv6 through IPv4 is using an IPsec VPN tunnel between to FortiGate devices. FortiOS supports IPv6 over IPsec. In this sort of scenario, 2 networks using IPv6 behind FortiGate units are separated by the Internet, which uses IPv4. An IPsec VPN tunnel is created between the 2 FortiGate units and a tunnel is created over the IPv4 based Internet but the traffic in the tunnel is IPv6. This has the additional advantage of make the traffic secure as well.

NAT

NAT or Network Address Translation is the process that enables a single device such as a router or firewall to act as an agent between the Internet or Public Network and a local or private network. This “agent”, in real time, translates the source IP address of a device on one network interface, usually the Internal, to a different IP address as it leaves another interface, usually the interface connected to the ISP and the Internet. This enables a single public address to represent a significantly larger number of private addresses.

NAT64 and NAT46

NAT64 and NAT46 are the terms used to refer to the mechanism that allows IPv6 addressed hosts to communicate with IPv4 addressed hosts and vice-versa. Without such a mechanism an IPv6 node on a network such as a corporate LAN would not be able to communicate with a web site that was still in a IPv4 only environment and IPv4 environments would not be able to connect to IPv6 networks.

One of these setups involves having at least 2 interfaces, 1 on an IPv4 network and 1 on an IPv6 network. The NAT64 server synthesizes AAAA records, used by IPv6 from A records used by IPv4. This way client-server and peer to peer communications will be able to work between an IPv6 only client and an IPv4 server without making changes to either of the end nodes in the communication transaction. The IPv6 network attached to the FortiGate unit should be a 32 bit segment, (for instance 64:ff9b::/96, see RFC 6052 and RFC 6146). IPv4 address will be embedded into the communications from the IPv6 client.

Because the IPv6 range of addresses is so much larger than the IPv4 range, a one to one mapping is not feasible. Therefore the NAT64 function is required to maintain any IPv6 to IPv4 mappings that it synthesizes. This can be done either statically by the administrator or automatically by the service as the packets from the IPv6 network go through the device. The first method would be a stateless translation and the second would be a stateful translation. NAT64 is designed for communication initiated from IPv6 hosts to IPv4 addresses. It is address mapping like this that allows the reverse to occur between established connections. The stateless or manual method is an appropriate solution when the NAT64 translation is taking place in front of legacy IPv4 servers to allow those specific servers to be accessed by remote IPv6-only clients. The stateful or automatic solution is best used closer to the client side when you have to allow some specific IPv6 clients to talk to any of the IPv4-only servers on the Internet.

There are currently issues with NAT64 not being able to make everything accessible. Examples would be SIP, Skype, MSN, Goggle talk, and sites with IPv4 literals. IPv4 literals being IPv4 addresses that are imbedded into content rather than a FQDN.

Policies that employ NAT64 or NAT46 can be configured from the web-based manager as long as the feature is enabled using the Features setting found at **System > Config > Features**.

- To create a NAT64 policy go to **Policy > Policy > NAT64 Policy** and select **Create New**.
- To create a NAT46 policy go to **Policy > Policy > NAT46 Policy** and select **Create New**.

The difference between these NAT policies and regular policies is that there is no option to use the security profiles and sensors.

NAT66

NAT 66 is Network Address Translation between 2 IPv6 network. The basic idea behind NAT 66 is no different than the regular NAT between IPv4 networks that we are all used to. The difference are in the mechanics of how it is performed, mainly because of the complexity and size of the addresses that are being dealt with.

In an IPv4 world, the reason for the use of NAT was usually one or a combination of the following 3 reasons:

- Improved security - actual addresses behind NAT are virtually hidden
- Amplification of addresses - hundreds of computers can use as little as a single public IP address
- Internal address stability - there is control of internal addressing. The addresses can stay the same even if Internet Service Providers change.

In these days of security awareness the protective properties of NAT are not something that are not normally depended on by themselves to defend a network and with the vastly enlarged IPv6 address scope there is no longer a need to amplify the available addresses. However, the desire to have internal address control still exists. The most common reason for using NAT66 is likely to be the maintaining of the existing address scheme of the internal network despite changes outside of it. Imagine that you have an internal network of 2000 IP addresses and one day the company changes its ISP and thus the addresses assigned to it. Even if most of the addressing is handled by DHCP, changing the address scheme is going to have an impact on operations.

Addressing stability can be achieved by:

- Keeping the same provider - this would depend on the reason for the change. If the cost of this provider has become too expensive this is unlikely. If the ISP is out of business it becomes impossible.
- Transfer the addresses from the old provider to the new one - There is little motivation for an ISP to do you a favor for not doing business with them.
- Get your own autonomous system number - this can be too expensive for smaller organizations.
- NAT - this is the only one on the list that is in the control of IT.

There are differences between NAT66 and IPv4 NAT. Because there is no shortage of addresses most organizations will be given a /48 network that can be translated into another /48 network. This allows for a one to one translation, no need for port forwarding. This is a good thing because port forwarding is more complicated in IPv6. In fact, NAT66 will actually just be the rewriting of the prefix on the address.

Example

If your current IPv6 address is

```
2001:db8:cafe::/48
```

you could change it to

```
2001:db8:fea7::/48
```

There is an exception to the one to one translation. NAT66 cannot translate internal networks that contain 0xffff in bits 49 through 63 - this is due to the way checksums are calculated in TCP/IP: they use the one's-complement representation of numbers which assigns the value zero to both 0x0000 and 0xffff.

How FortiOS differentiates sessions when NATing

The basics of NAT are fairly simple. Many private addresses get translated into a smaller number of public addresses, often just one. The trick is how the FortiGate keeps track of the return traffic because the web server, or what ever device that was out on the Internet is going to be sending traffic back not to the private address behind the FortiGate but to the IP address of the interface on the public side of the FortiGate.

The way this is done is by making each session unique. Most of the attributes that are available in the network packets cannot be changed without changing where the packet will go but because the source port has to be changed anyway in case two computer on the network used the same source port this is a useful way of making each listing of network attributes a unique combination. As a packet goes through the NAT process FortiOS assigns different source ports for each of the internally initiated sessions and keeping track of which port was used for each device in a database until the session has ended. It then becomes a matter of how the port number is selected.

In a very simple example of an environment using NAT, we will use a fictitious university with a rather large student population. So large in fact that they use a subnet of `10.0.0.0/8` as their subnet for workstation IP addresses. All of these private IP addresses are NATed out a single IP address. To keep the number of numeric values in this example from getting to a confusing level, we'll just us "`u.u.u.1`" to refer to the public IP address of the University and the IP address of the web server on the Internet will be "`w.w.w.1`".

Student A (IP address `10.1.1.56`) sends an HTML request to a web server on the Internet with the IP address `w.w.w.1`. The applicable networking information in the packet breaks down as follows:

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	`10.1.1.56`	`u.u.u.1`
Destination IP address or dst-ip:	`w.w.w.1`	`w.w.w.1`
Source port or src-port:	10000	**46372**
Destination port or dst-port	80	80

The source IP address is now that of the public facing interface of the FortiGate and source port number is an unused TCP port number on the FortiGate chosen by the FortiGate. Of these variable the only one the that FortiGate can really change and still have the packet reach the correct destination, in both directions, is the source port number.

There are a few methods of assigning the port number. First we'll look at the methods that are or have been used in the industry but aren't used by Fortinet.

Global pool

This method of differentiation focuses on the attribute of the source port number. In this approach a single pool of potential port numbers is set aside for the purposes of NAT. As a pool number is assigned, it is removed from the pool so that two sessions from different computers can not using the same port number. Once the session is over and no longer in use by the computer, the port number is put back into the pool where it can be assigned again.

Example global pool:

	Hexidecimal	Decimal
Start or range	0x7000	28672
End end of range	0xF000	61440
Possible ports in range	215	32768

This is a simple approach to implement and is good if the number of connections in unlike to reach the pool size. It would be okay for home use, but our example is for a university using `10.1.1.0/8` as a subnet. That means 16,777,214 possible IP addresses; more than this method can handle.

Fortinet does not use this method.

Global per protocol

This method uses the attributes source port number and type of protocol to differentiate between sessions.This approach is a variation of the first one. An additional piece of information is refered to in the packet that describes the protocol. For instance UDP or TCP. This could effectively double the number of potential addresses to NAT.

Example:

Here are two possible packets that would be considered different by the FortiGate so that any responses from the web server would make it back to their correct original sender.

From Student A

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	10.1.1.56	u.u.u.1
Destination IP address or dst-ip:	w.w.w.1	w.w.w.1
Protocol	tcp	tcp
Source port or src-port:	10000	**46372**
Destination port or dst-port	80	80

From Student B

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	10.5.1.233	u.u.u.1
Destination IP address or dst-ip:	w.w.w.1	w.w.w.1
Protocol	udp	udp
Source port or src-port:	26785	**46372**
Destination port or dst-port	80	80

Even though the source port is the same, because the protocol is different they are considered to be from different sessions and different computers.

The drawback is that it would depend on the protocols being used be evenly distributed between TCP and UDP. Even if this was the case the number would only double; reaching an upper limit of 65,536 possible connections. That number is still far short of the possible more than 16 million for an IP subnet with an eight bit subnet mask like the one in our example.

Fortinet does not use this method.

Per NAT IP Pool

This approach adds on to the previous one by adding another variable. In this case that variable is the IP addresses on the public side of the FortiGate. By having a pool of IP addresses to assign as the source IP address when NATing, the same number that was potentially available for the Global per protocol method can be multiplied by the number of external IP addresses in the pool. If you can assign a second IP address to the pool, you can double the potential number of sessions.

Example:

In this example it will be assumed that the FortiGate has 2 IP addresses that it can use. This could happen either by using two ISPs, or by having a pool of IP addresses assigned to a single interface. For simplicity will will refer

to these IP public IP addresses as `u.u.u.1` and `u.u.u.2`.

Here are two possible packets that would be considered different by the FortiGate so that any responses from the web server would make it back to their correct original sender.

From Student A

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	`10.1.1.56`	`u.u.u.1`
Destination IP address or dst-ip:	`w.w.w.1`	`w.w.w.1`
Protocol	tcp	tcp
Source port or src-port:	10000	**46372**
Destination port or dst-port	80	80

From Student B

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	`10.5.1.233`	`u.u.u.2`
Destination IP address or dst-ip:	w.w.w.1	w.w.w.1
Protocol	tcp	tcp
Source port or src-port:	26785	**46372**
Destination port or dst-port	80	80

In this example we even made the protocl the same. After the NATing process all of the variables are the same except the sourse addresss. This is still going to make it bake to the original sender.

The drawback is that if you have only one IP address for the purposes of NATing this method does not gain you anything over the last method. Or if you do have multiple IP addresses to use it will still take quite a few to reach the 16 million possible that the subnet is capable of handling.

Fortinet does not use this method.

Per NAT IP, destination IP, port, and protocol

This is the approach that FortiOS uses.

It uses all of the differentiation point of the previous methods, NAT IP, port number and protocol, but the additonal information point of the destination IP is also used. So now the network information points in the packet that the FortiGate keeps in its database to differentiate between sessions is:

- Public IP address of the FortiGate assigned by NATing
- Protocol of the traffic
- Source port assigned by the FortiGate
- Destination IP address of the packet

The last one is an especially good way to differentiate because as a theortical number, the upper limit on that is the numbers of Public IP addresses on the whole of the Internet. Chances are that while a large number of session from inside the University will be going to a small group of sites such as Google, Youtube, Facebook and some others it is unlikely that they will all be going to them at the same time.

Example:

In this example it will be assumed that the FortiGate has only one IP address.Two possible packets will be described. The only difference in the attributes recorded will be the destination of the HTML request.These packets are still considered to be from differnt sessions and any responses will make it back to the correct computer.

From Student A

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	10.1.1.56	u.u.u.1
Destination IP address or dst-ip:	w.w.w.1	w.w.w.1
Protocol	tcp	tcp
Source port or src-port:	10000	**46372**
Destination port or dst-port	80	80

From Student B

Attribute	Original Packet	Packet after NATing
Source IP address or src-ip	10.5.1.233	u.u.u.1
Destination IP address or dst-ip:	w.w.w.2	w.w.w.2
Protocol	tcp	tcp
Source port or src-port:	26785	**46372**
Destination port or dst-port	80	80

The reason that these attributes are used to determine defferentiation between traffic is based on how the indexes for the sessions are recorded in the database. When a TCP connection is made through a FortiGate unit, a session is created and two indexes are created for the session. The FortiGate unit uses these indexes to guide matching traffic to the session.

This following could be the session record for the TCP connection in the first example.

Attribute	Outgoing Traffic	Returning Traffic
Source IP address	10.78.33.97 (internal address)	w.w.w.1
Destination address	w.w.w.1	u.u.u.1
Protocol	tcp	tcp
Source port	10000 (from original computer) 46372 (assigned by NAT)	80
Destination port	80	46372 (FortiGate assigned port)

Using the FortiGate's approach for session differentiation, FortiOS only has to ensure that the assigned port, along with the other four attributes is a unique combination to identify the session. So for example, if Student A simultaneously makes a HTTP(port 80) connection and a HTTPS(port 443) connection the same web server this would create another session and the index in the reply direction would be:

Attribute	Outgoing Traffic	Returning Traffic
Source IP address	10.78.33.97 (internal address)	w.w.w.1
Destination address	w.w.w.1	u.u.u.1
Protocol	tcp	tcp
Source port	10000 (from original computer) 46372 (assigned by NAT)	443
Destination port	443	46372 (FortiGate assigned port)

These two sessions are different and acceptable because of the different source port numbers on the returning traffic or the destination port depending on the direction of the traffic.

Calculations for possible session numbers

The result of using these four attributes instead of just the one that was originally used is a large increase in the number of possible unique combinations.For those who love math, the maximum number of simultaneous connections that can be supported is:

N x R x P x D x Dp

where:

- **N** is the number of NAT IP addresses
- **R** is the port range,
- **P** is the number of protocols,
- **D** is the number of unique destination IP addresses
- **Dp** the number of unique destination ports.

As a rough example let's do some basic calculations

- N - In our existing example we have already stated that there is only one public IP address that is being used by NAT. Realistically, for a university this number would likely be larger, but we're keeping it simple.

  N = 1

R - The port range for our example has already been describe and we will keep it the same.

R = 32768

P - While there are a few protocols that are involved in Internet traffic we will limit this calculation just to TCP traffic.

P = 1

D - As mentioned before the number of unique destination addresses is growing larger every day,so figureing out the upper limit of that numbe would be difficult to say the least. Instead we will make the assumption that most of the university students, do to their shared interest and similar demographic will concentrate most of their web browsing to the same sites; sites such as YouTube, Facebook, Google, Twitter, Instagram, Wikipedia etc. This is not even taking into account the fact that many of these popular sites use load balancing and multiple IP addresses. As an arbatrary number let's use the number 25.

D = 25

Dp - To keep things simple it is tempting to limit the destiation port to port 80, the one that many associate with web browsing, but this would not be realistic. the use of HTTPS, port 443 is on the rise. There is also email, DNS, FTP, NTP and a number of other background services that we use without thinking too closely about. Let's keep it small and say ten of them.

Dp = 10

The math on this very conservative calculation is:

1 x 32768 x 1 x 25 x 10 = 8,192,000 possible NAT sessions

When you take into account that the chances of everybody being online at the same time, going only to one of those 25 sites and not millions of others, and using only TCP not UDP or any of the other protocols, it starts to look like this method may provide enough potential unique sessions even for a subnet as large as the one described.

How packets are handled by FortiOS

To give you idea of what happens to a packet as it makes its way through the FortiGate unit here is a brief overview. This particular trip of the packet is starting on the Internet side of the FortiGate firewall and ends with the packet exiting to the Internal network. An outbound trip would be similar. At any point in the path if the packet is going through what would be considered a filtering process and if fails the filter check the packet is dropped and does not continue any further down the path.

This information is covered in more detail in other in the Troubleshooting chapter of the FortiOS Handbook in the Life of a Packet section.

The incoming packet arrives at the external interface. This process of entering the device is referred to as **ingress**.

Step #1 - Ingress

1. Denial of Service Sensor
2. IP integrity header checking
3. IPsec connection check
4. Destination NAT
5. Routing

Step #2 - Stateful inspection engine

1. Session Helpers
2. Management Traffic
3. SSL VPN
4. User Authentication
5. Traffic Shaping
6. Session Tracking
7. Policy lookup

Step #3 - Security profiles scanning process

1. Flow-based Inspection Engine
2. IPS
3. Application Control
4. Data Leak Prevention
5. Email Filter
6. Web Filter
7. Anti-virus
8. Proxy-based Inspection Engine
9. VoIP Inspection
10. Data Leak Prevention
11. Email Filter
12. Web Filter
13. Anti-virus
14. ICAP

Step #4 - Egress

1. IPsec
2. Source NAT
3. Routing

FortiGate modes

The FortiGate unit has a choice of modes that it can be used in, either NAT/Route mode or Transparent mode. The FortiGate unit is able to operate as a firewall in both modes, but some of its features are limited in Transparent mode. It is always best to choose which mode you are going to be using at the beginning of the set up. Once you start configuring the device, if you want to change the mode you are going to lose all configuration settings in the change process.

NAT/Route mode

NAT/Route mode is the most commonly used mode by a significant margin and is thus the default setting on the device. As the name implies the function of NAT is commonly used in this mode and is easily configured but there is no requirement to use NAT. The FortiGate unit performs network address translation before IP packets are sent to the destination network.

These are some of the characteristics of NAT/Route mode:

- Typically used when the FortiGate unit is a gateway between private and public networks.
- Can act as a router between multiple networks within a network infrastructure.
- When used, the FortiGate unit is visible to the networks that is connected to.
- Each logical interface is on a distinct subnet.
- Each Interface needs to be assigned a valid IP address for the subnet that it is connected to it.

Transparent mode

Transparent mode is so named because the device is effectively transparent in that it does not appear on the network in the way that other network devices show as a nodes in the path of network traffic. Transparent mode is typically used to apply the FortiOS features such as Security Profiles etc. on a private network where the FortiGate unit will be behind an existing firewall or router.

These are some of the characteristics of Transparent mode:

- The FortiGate unit is invisible to the network.
- All of its interfaces are on the same subnet and share the same IP address.
- The FortiGate unit uses a Management IP address for the purposes of Administration.
- Still able to use NAT to a degree, but the configuration is less straightforward

In Transparent mode, you can also perform NAT by creating a security policy or policies that translates the source addresses of packets passing through the FortiGate unit as well as virtual IP addresses and/or IP pools.

Quality of Service

The Quality of Service (QoS) feature allows the management of the level of service and preference given to the various types and sources of traffic going through the firewall so that the traffic that is important to the services and functions connecting through the firewall gets the treatment required to ensure the level of quality that is required. QoS can be helpful for organizations that are trying to manage their voice and streaming multi-media traffic, which can rapidly consume bandwidth. Both voice and streaming multi-media are sensitive to latency. FortiGate units support QoS using traffic policing, traffic shaping, and queuing.

Traffic policing

Packets are dropped that do not conform to bandwidth limitations

Traffic shaping

Assigning minimum levels of bandwidth to be allocated to specific traffic flows to guarantee levels of service or assigning maximum levels of bandwidth to be allocated to specific traffic flows so that they do not impede other flows of traffic.

This helps to ensure that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Traffic shaping also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instant in time. Flows that are greater than the maximum rate are subject to traffic policing.

Queuing

Assigning differing levels of priority to different traffic flows so that traffic flows that are adversely effected by latency are prevented from being effected by traffic flows that are not subject to the effects of latency. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.

An example of where you would want to use something like this is if you had competing traffic flows of Voice over IP traffic and email traffic. The VoIP traffic is highly susceptible to latency issues. If you have a delay of a few seconds it is quickly noticeable when it is occurring. Email on the other hand can have a time delay of much longer and it is highly unlikely that it will be noticed at all.

By default, the priority given to any traffic is high, so if you want to give one type of traffic priority over all other traffic you will need to lower the priority of all of the other traffic.

Interfaces and zones

A Firewall is a gateway device that may be the nexus point for more than 2 networks. The interface that the traffic is coming in on and should be going out on is a fundamental concern for the purposes of routing as well as security. Routing, policies and addresses are all associated with interfaces. The interface is essentially the connection point of a subnet to the FortiGate unit and once connected can be connected to other subnets.

Physical interfaces or not the only ones that need to be considered. There are also virtual interfaces that can be applied to security policies. VLANs are one such virtual interface. Interfaces if certain VPN tunnels are another.

Policies are the foundation of the traffic control in a firewall and the Interfaces and addressing is the foundation that policies are based upon. Using the identity of the interface that the traffic connects to the FortiGate unit tells the firewall the initial direction of the traffic. The direction of the traffic is one of the determining factors in deciding how the traffic should be dealt with. You can tell that interfaces are a fundamental part of the policies because, by default, this is the criteria that the policies are sorted by.

Zones are a mechanism that was created to help in the administration of the firewalls. If you have a FortiGate unit with a large number of ports and a large number of nodes in you network the chances are high that there is going to be some duplication of policies. Zones provide the option of logically grouping multiple virtual and physical FortiGate firewall interfaces. The zones can then be used to apply security policies to control the incoming and outgoing traffic on those interfaces. This helps to keep the administration of the firewall simple and maintain consistency.

For example you may have several floors of people and each of the port interfaces could go to a separate floor where it connects to a switch controlling a different subnet. The people may be on different subnets but in terms

of security they have the same requirements. If there were 4 floors and 4 interfaces a separate policy would have to be written for each floor to be allowed out on to the Internet off the WAN1 interface. This is not too bad if that is all that is being done, but now start adding the use of more complicated policy scenarios with Security Profiles, then throw in a number of Identity based issues and then add the complication that people in that organization tend to move around in that building between floors with their notebook computers.

Each time a policy is created for each of those floors there is a chance of an inconsistency cropping up. Rather than make up an additional duplicate set of policies for each floor, a zone can be created that combines multiple interfaces. And then a single policy can created that uses that zone as one side of the traffic connection.

Firewall objects

As was mentioned earlier, the components of the FortiGate firewall go together like interlocking building blocks. The Firewall objects are a prime example of those building blocks. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the FortiGate unit easier and more intuitive as well as easier to change. By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change.

This chapter includes information about the following Firewall objects:

- Addresses
- Services and TCP ports
- Firewall schedules
- Security profiles

UUID support

A Universally Unique Identified (UUID) attribute has been added to some firewall objects, so that the logs can record these UUID to be used by a FortiManager or FortiAnalyzer unit. The objects currently include:

- Addresses, both IPv4 and IPv6
- Address Groups, both IPv4 and IPv6
- Virtual IPs, both IPv4 and IPv6
- Virtual IP groups, both IPv4 and IPv6
- Policies, IPv4,IPv6 and IP64

A UUID is a 16-octet (128-bit) number that is represented by 32 lowercase hexidecimal digits. The digits are displayed in five groups separated by hyphens (-). The pattern is 8-4-4-4-12; 36 digits if you include the hyphens.

Note: UUID is only supported on large-partition platforms (>=128M)

Addresses

Firewall addresses define sources and destinations of network traffic and are used when creating policies. When properly set up these firewall objects can be used with great flexibility to make the configuration of firewall policies simpler and more intuitive. The FortiGate unit compares the IP addresses contained in packet headers with a security policy's source and destination addresses to determine if the security policy matches the traffic.

The addresses in the FortiGate unit can include:

- IPv4 addresses
- IPv6 addresses
- IPv4 Address Groups
- IPv6 Address Groups

- IP Pools
- Virtual IP Addresses
- Geography based addresses
- Wildcard addresses and netmasks
- Fully Qualified Domain Name addresses
- Multicast addresses

Interfaces

When setting up an address one of the parameters that is asked for is the interface. This means that the system will expect to see that address only on the interface that you select. You can only select one interface. If you expect that the address may be seen at more than one interface you can choose the “any” interface option. Whenever, possible it is best to choose a more specific interface than the “any” option because in the GUI configuration of firewall policies there is a drop down field that will show the possible addresses that can be used. The drop down will only show those addresses that can be on the interface assigned for that interface in the policy.

Example:

- You have an address called “XYZ”.
- “XYZ” is set to the WAN1 interface because that is the only interface that will be able to access that address.
- When you are selecting a Source Address in the Web-based Manager for a policy that is using the DMZ the address “XYZ” will not be in the drop-down menu.

When there are only 10 or 20 addresses this is not a concern, but if there are a few hundred addresses configured it can make your life easier.

Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, the address cannot be deleted until it is deselected from the policy.

Addressing Best Practices Tip

The other reason to assign a specific interface to addresses is that it will prevent you from accidentally assigning an address where it will not work properly. Using the example from earlier, if the “XYZ” address was assigned to the “Any” interface instead of WAN1 and you configure the “XYZ” address.

IPv4 addresses

When creating an IPv4 address there are a number of different types of addresses that can be specified. These include:

- Subnet
- IP Range
- FQDN
- Geography
- URL Pattern (Explicit Proxy)

Which one chosen will depend on which method most easily yet accurately describes the addresses that you are trying to include with as few entries as possible based on the information that you have. For instance, if you are trying to discribe the addresses of a specific company’s web server but it you have no idea of how extensive there

webserver farm is you would be more likely to use a Fully Qualified Domain Name (FQDN) rather than a specific IP address. On the other hand some computers don't have FQDNs and a specific IP address must be used.

The following is a more comprehesive description of the differnt types of addresses.

Subnet addresses

The subnet type of address is expressed using a host address and a subnet mask. From a strickly mathematical stand point this is the most flexible of the types because it can refer to as little as the address for one computer or as many as all of them.

It is usally used when refering to your own internal addresses because you know what they are and they are usually administered in groups that are nicely deferentiated along the lines of the old A, B, and C classes of IPv4 addresses. They are also addresses that are not likely to change with the changing of Internet Service Providers (ISP).

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a firewall address can be:

- A single host such as a single computer with the address 192.45.46.45
- A range of hosts such as all of the hosts on the subnet 192.45.46.1 to 192.45.46.255
- All hosts, represented by 0.0.0.0 which matches any IP address

The netmask corresponds to the subnet class of the address being added, and can be represented in either dotted decimal or CIDR format. The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format. Example formats:

- Netmask for a class A subnet of 16,777,214 usable addresses: 255.0.0.0, or /8
- Netmask for a class B subnet of 65,534 usable addresses: 255.255.0.0, or /16
- Netmask for a class C subnet of 254 usable addresses: 255.255.255.0, or /24
- Netmask for subnetted class C of 126 usable addresses: 255.255.255.128, or /25
- Netmask for subnetted class C of 62 usable addresses: 255.255.255.128, or /26
- Netmask for subnetted class C of 30 usable addresses: 255.255.255.128, or /27
- Netmask for subnetted class C of 14 usable addresses: 255.255.255.128, or /28
- Netmask for subnetted class C of 6 usable addresses: 255.255.255.128, or /29
- Netmask for subnetted class C of 2 usable addresses: 255.255.255.128, or /30
- Netmask for a single computer: 255.255.255.255, or /32
- Netmask used with 0.0.0.0 to include all IP addresses: 0.0.0.0, or /0

So for a single host or subnet the valid format of IP address and netmask could be either:

x.x.x.x/x.x.x.x, such as 192.168.1.0/255.255.255.0

or

x.x.x.x/x, such as 192.168.1.0/24

Creating a subnet address

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**.
   - If you use the down arrow next to **Create New**, select **Address**.

3. Choose the **Category, "Address".**
4. Input a **Name** for the address object.
5. Select the **TypeSubnet** from the dropdown menu.
6. Input the host address and subnet mask in the **Subnet / IP Range** field.
7. Select the **Interface** from the dropdown menu.
8. Check the **Visibility** box.
9. Input any additional information in the **Comments** field.
10. Press **OK.**

Example

Example of a Subnet address for a database server on the DMZ:

Category	Address
Name	DB_server_1
Type	Subnet
Subnet / IP Range	192.168.50.26
Interface	DMZ
Visibility	[checked]
Comments	Database server used by public facing company webservers

IP range addresses

Where the Subnet address is good a representing a standardized group of addresses that are subnets the IP Range type of address can describe a group of addresses while being specific and granular. It does this by specifying a continuous set of IP addresses between one specific IP address and another. While it is most common that this range is with a subnet it is not a requirement. For instance, 192.168.1.0/24 and 192.168.2.0/24 would be 2 separate subnets but if you wanted to descript the top half of one and the bottom half of the other you could describe the range of 192.168.1.128-192.168.2.127. It's also a lot easier that trying to calculate the correct subnet mask.

The format would be:

x.x.x.x-x.x.x.x, such as 192.168.110.100-192.168.110.120

There is a notation that is commonly used and accepted by some devices that follows the format:

x.x.x.[x-x], such as 192.168.110.[100-120]

This format is not recognized in FortiOS 5.2 as a valid IP Range.

Creating a IP range address

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**.

- If you use the down arrow next to **Create New**, select **Address**.

3. Choose the **Category, "Address".**
4. Input a **Name** for the address object.
5. Select the **TypeIP Range** from the dropdown menu.
6. Input the host address and subnet mask in the **Subnet / IP Range** field.
7. Select the **Interface** from the dropdown menu.
8. Check the **Visibility** box.
9. Input any additional information in the **Comments** field.
10. Press **OK.**

Example

Example of a IP Range address for a group of computers set aside for guests on the company network.

Category	Address
Name	Guest_users
Type	IP Range
Subnet / IP Range	192.168.100.200-192.168.100.240
Interface	Port1
Visibility	[checked]
Comments	Computers on the 1st floor used by guests for Internet access.

IP Range addresses can now be configured for IPv6 addresses. The only differences in creating an IPv6 IP Range address is that you would choose IPv6 Address for the Category and the syntax of the address in the Subnet/IP Range field would be in the format of 2001:0db8:0000:0002:0:0:0:20-2001:0db8:0000:0004:0:0:0:20

FQDN addresses

By using Fully Qualified Domain Name (FQDN) addressing you can take advantage of the dynamic ability of the service to keep up with address changes without having to manually change the addresses on the FortiGate. FQDN addresses are most often used with external web sites but they can be used for internal web sites as well if there is a trusted DNS server that can be accessed. FQDN addressing also comes in handy for large web sites that may use multiple addresses and load balancers for their web sites. The FortiGate firewall automatically maintains a cached record of all the addresses resolved by the DNS for the FQDN addresses used.

For example, if you were doing this manually and you wanted to have a security policy that involved Google you could track down all of the IP addresses that they use across multiple countries. Using the FQDN address is simpler and more convenient.

When representing hosts by an FQDN, the domain name can also be a subdomain, such as mail.example.com.

Valid FQDN formats include:

- <host_name>.<top_level_domain_name> such as example.com
- <host_name>.<second_level_domain_name>.<top_level_domain_name>, such as mail.example.com

When creating FQDN entries it is important to remember that:

- Wildcards are not supported in FQDN address objects
- While there is a level of convention that would imply it, “www.example.com” is not necessarily the same address of “example.com”. they will each have their own records on the DNS server.

The FortiGate firewall keeps track of the DNS TTLs so as the entries change on the DNS servers the IP address will effectively be updated for the FortiGate. As long as the FQDN address is used in a security policy, it stores the address in the DNS cache.

There is a possible security downside to using FQDN addresses. Using a fully qualified domain name in a security policy means that your policies are relying on the DNS server to be accurate and correct. DNS servers in the past were not seen as potential targets because the thinking was that there was little of value on them and therefore are often not as well protected as some other network resources. People are becoming more aware that the value of the DNS server is that in many ways it controls where users and computers go on the Internet. Should the DNS server be compromised, security policies requiring domain name resolution may no longer function properly.

Creating a Fully Qualified Domain Name address

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**.
   - If you use the down arrow next to **Create New**, select **Address**.
3. Choose the **Category, “Address”.**
4. Input a **Name** for the address object.
5. Select the **TypeFQDN** from the dropdown menu.
6. Input the domain name in the **FQDN** field.
7. Select the **Interface** from the dropdown menu.
8. Check the **Visibility** box.
9. Input any additional information in the **Comments** field.
10. Press **OK.**

Example

Example of a FQDN address for a remote FTP server used by Accounting team:

Category	Address
Name	Payroll_FTP_server
Type	FQDN
FQDN	ftp.payrollcompany.com
Interface	any
Visibility	[checked]
Comments	Third party FTP server used by Payroll.

Geography based addresses

Geography based addressing enables you to design policies based on addresses that are associated with a country.

This feature can be used to make either inclusive or exclusive policies. For instance, if you have a SSL VPN where the users will only be connecting from a single country, but you don't know from where in that country, you can filter out any connections coming in that are from outside that country.

On the other side of the equation, if you find that you are constantly being attacked by malicious intruders from a few countries that you have no dealings with you can block access to them before any traffic comes through.

The matching of geographical country designations to an IP address is achieved by collecting data from any IP addresses that connect to any of the FortiGuard Servers throughout the world. As a secondary task, when a FortiGuard server connects to an IP it also does a search on the Country of origin for the address and updates the database.

There is no single comprehensive list of IP addresses and their locations available because IP addresses can be transferred between ISPs or countries and some organization may not keep complete or up-to-date records regarding locations. FortiGuard Services are constantly updating their database of addresses matched to locations, but the database is dynamic and there may be addresses that have not been resolved to a location. While this means that there can be gaps in the completeness of the database it is possible to fill them in manually by means local to your FortiGate unit.

FortiOS IPv6 does not support the creation of geography-based address objects. This feature is for IPv4 addresses only.

Best Practices Tip:

Based on the limitation of the IP address matched to country database, it is best to use this type of address in a group with other addresses to fill in the gaps. For instance, if you are a company in Country "A" and all of your employees that will be using the SSL-VPN connection are in that country, the best practice would be to create an address group that includes the geographical address of Country "A". As valid addresses appear that are not allowed, you can add these other IPs to that group using IP addresses or IP range addresses without having to change the policy itself.

If you are trying to block addresses the principle works just the same. Your logs show that someone from IP address x.x.x.x has been trying to connect inappropriately to your network. You use a IP locator web site to determine that they have been attempting to connect from Country “X”. Up until now they have not been successful, but you don’t deal with the country they are connecting from so don’t mind blocking the whole country. Create an address group that is designed for Blocking Access to any addresses in it, then add the geographical address for Country “X”. Even if the policy does not block every single IP address from that country you have greatly increased your odds of blocking potential intrusion attempts. As your logs show other attempts you can look them up in an IP locator web site and if they are from the same country you can add the IP address for the subnet that they are connecting from.

Creating a geography address

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**.
   - If you use the down arrow next to **Create New**, select **Address**.
3. Choose the **Category, “Address”.**
4. Input a **Name** for the address object.
5. Select the **Type,Geography** from the dropdown menu.
6. Select the country from the dropdown menu in the **Country** field.

   The bottom of the dropdown menu has a search field so that you don’t have to scroll through the entire list of countries.
7. Select the **Interface** from the dropdown menu.
8. Check the **Visibility** box.
9. Input any additional information in the **Comments** field.
10. Press **OK.**

Example

Example of a Geography address for a country that should be able to access resourses on the network.

Category	Address
Name	United States
Type	Geography
Country	United States
Interface	any
Visibility	[checked]
Comments	

Configuring the address in the CLI

Enter the following CLI commands:

```
config firewall address
   edit Cuba
      set type geography
      set country CN
      set interface wan1
   end
```

Overrides

It is possible to assign a specific ip address range to a customized country ID. Generally, geographic addressing is done at the VDOM level; it could be considered global if you are using the root VDOM, but the geoip-override setting is a global setting.

```
config system geoip-override
   edit "test"
      set country-id "A0"
         config ip-range
            edit 1
               set start-ip 7.7.7.7
               set end-ip 7.7.7.8
               next
            edit 2
               set start-ip 7.7.10.1
               set end-ip 7.7.10.255
               end
```

- While the setting exists in the configuration file, the system assigns the country-id option automatically.
- While you can use "edit 1" and "edit 2", it is simpler to use "edit 0" and let the system automatically assign an ID number.

After creating a customized Country by using geoip-override command, the New country name has been added automatically to the country list and will be available on the Firewall Address Country field.

URL pattern addresses

This address is different from the other addresses in that it is not designed to be used in the normal firewall policy configuration. It is intended to be used only with explicit web proxies, and then only as a destination. In some respects it is like a FQDN address in that it uses DNS to look up the IP address that represents but it then goes a little more granular and further filters by the URL that is used to specify a location within the website itself. Wildcard characters can even be used to keep the address from being too granular.

Creating a IP range address

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**.
   - If you use the down arrow next to **Create New**, select **Address**.
3. Choose the **Category, “Address”.**
4. Input a **Name** for the address object.
5. Select the **Type,URL Pattern (Explicit Proxy)** from the dropdown menu.
6. Enter the URL value.

7. Select the **Interface** from the dropdown menu.
8. Check the **Visibility** box.
9. Input any additional information in the **Comments** field.
10. Press **OK.**

Example

Example of a URL pattern address for a wiki on the example.com website.

Category	Address
Name	Example.com_wiki
Type	URL Pattern (Explicit Proxy)
URL Pattern	example.com/wiki/*
Interface	any
Visibility	[checked]
Comments	<optional>

Address groups

Address groups are designed for ease of use in the administration of the device. If you have a number of addresses or address ranges that will commonly be treated the same or require the same security policies, you can put them into address groups, rather than entering multiple individual addresses in each policy refers to them.

The use of groups is not required. If you have a number of different addresses you could add them individually to a policy and the FortiGate firewall will process them just as quickly and efficiently as if they were in a group, but the chances are that if you have used a group once you could need to use it again and depending on the number of addresses involved entering them individually for each policy can become tedious and the likelihood of an address being missed becomes greater. If you have a number of policies using that combination of addresses it is much easier to add or subtract addresses from the group than to try and remember all of the firewall policies that combination of addresses was used in. With the group, you only have to make the one edit and it is used by any firewall policy using that address group.

Because security policies require addresses with homogenous network interfaces, address groups should contain only addresses bound to the same network interface, or to Any.

For example, if address 1.1.1.1 is associated with port1, and address 2.2.2.2 is associated with port2, they cannot be in the same group. However, if 1.1.1.1 and 2.2.2.2 are configured with an interface of Any, they can be grouped, even if the addresses involve different networks.

IPv4 address groups and IPv6 address groups are created and treated separately. You cannot mix IPv4 firewall addresses and IPv6 firewall addresses in the same address group. Because the Internet is currently based on IPv4 addresses IPv6 address groups cannot include FQDN or Geography based addresses.

Creating an address group

The method for creating either a IPv4 group or an IPv6 group is idential except for the selection of **Type**.

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select the down arrow next to Create New, select **Address Group**.
3. Choose the **Type,** that is applicable to the proposed sellection of addresses**.**
4. Input a **Group Name** for the address object.
5. Check the **Show in Address List** box.
6. Next to **Members** there is a dropdown menu that can be used to select from the available Address objects. It is possible to select more than 1 entry. Just select the green plus sign next to the field to add an additional entry. Select the “X” icon in the field to remove an entry.
7. Input any additional information in the **Comments** field.
8. Press **OK.**

UUID support

Syntax:

```
config firewall {address|addres6|addgrp|addgrp6}
   edit 1
      set uuid <example uuid: 8289ef80-f879-51e2-20dd-fa62c5c51f44>
      next
   end
```

Virtual IPs

The mapping of a specific IP address to another specific IP address is usually referred to as Destination NAT. FortiOS has a component that is a bit more specialized along this line called a Virtual IP Address, sometimes referred to as a VIP. FortiOS uses a Virtual IP address to map an External IP address to an IP address. This address does not have to be an individual host, it can also be an address range. This mapping can include all TCP/UDP ports or if Port Forwarding is enabled it will only refer to the specific ports configured.

Virtual IP addresses are typically used to NAT external or Public IP addresses to internal or Private IP addresses. Using a Virtual IP address between 2 internal Interfaces made up of Private IP addresses is possible but there is rarely a reason to do so as the 2 networks can just use the IP addresses of the networks without the need for any address translation. Using a Virtual IP address for traffic going from the inside to the Internet is even less likely to be a requirement, but it is supported.

Something that needs to be considered when there are multiple Public IP addresses on the external interface(s) is that when a Virtual IP address is used without Port Forwarding enabled there is a reciprocal effect as far as traffic flow is concerned. Normally, on a firewall policy where NAT is enabled, for outgoing traffic the internal address is translated to the Public address that is assigned to the FortiGate, but if there is a Virtual IP address with no port forwarding enabled, then the Internal IP address in the Mapped field would be translated to the IP address configured as the External Address in the VIP settings.

Best practice: Put any policies with a VIP right at the beginning of the policy list, with nothing before them. VIP traffic is processed first, before the regular rules of order in policies are applied. The sequence of the policies not containing VIPS will not effect those that do contain VIPS, regardless of the order they are in. Put VIP policies before any others to remind yourself of where they really are in the sequence. For more on this topic, read the "Exception to policy order" on page 1009.

Example

- The assigned External address (WAN1) of the FortiGate unit is 172.12.96.3 with a subnet mask of 255.255.255.128
- There is a Virtual IP address set up to map the external address 172.12.96.127 on WAN1 to the internal IP address of 192.168.1.127
- Port Forwarding is not enabled because you want all allowed traffic going to the external IP address to go to this server.

In this case any outbound traffic from 192.168.1.127 will go out on WAN1 with the IP address of 172.12.96.127 as the source IP address.

In terms of actually using the Virtual IP address, they would be using in the security policies in the same places that other addresses would be used, usually as a Destination Address.

UUID support for VIP

UUID is now supported in for virtual IPs and virtual IP groups. This includes virtual IPs for IPv4, IPv6, NAT46, and NAT64. To view the UUID for these objects in a FortiGate unit's logs, log-uuid must be set to extended mode, rather than policy-only (which only shows the policy UUID in a traffic log). UUID can only be configured through the CLI

Syntax:

```
config sys global
   set log-uuid {disable | policy-only | extended}
end
```

There is another type of address that the term “virtual IP address” commonly refers to which is used in load balancing and other similar configurations. In those cases, a number of devices share a separately created virtual IP address that can be sent to multiple possible devices. In FortiOS these are referred to as Virtual Servers and are configured in the “Load Balance” section.

Dynamic VIP according to DNS translation

When a dynamic virtual IP is used in a policy, the dynamic DNS translation table is installed along with the dynamic NAT translation table into the kernel. All matched DNS responses will be translated and recorded regardless if they hit the policy. When a client request hits the policy, dynamic NAT translation will occur if it matches a record, otherwise the traffic will be blocked.

Syntax

```
config firewall vip
   edit "1"
      set type dns-translation
      set extip 192.168.0.1-192.168.0.100
      set extintf "dmz"
      set dns-mapping-ttl 604800
      set mappedip "3.3.3.0/24" "4.0.0.0/24"
      end
   end
```

Creating a virtual IP

1. Go to **Policy & Objects > Objects > Virtual IPs.**
2. Select **Create New**.
   - If you use the down arrow next to Create New, select **Virtual IP**.
3. Choose the **VIP Type.**

   The options available are:

   a. IPv4 VIP - IPv4 on both sides of the FortiGate Unit.

   b. IPv6 VIP - IPv6 on both sides of the FortiGate Unit.

   c. NAT46 VIP - Going from an IPv4 Network to an IPv6 Network.

   d. NAT64 VIP - Going from an IPv6 Network to an IPv4 Network.

   Which is chosen will depend on which of the IP version networks is on the external interface of the FortiGate unit and which is on the internal interface.
4. Input a **Name** for the Virtual IP.
5. Input any additional information in the **Comments** field.
6. Using the dropdown menu for the Interface Field, choose the incoming interface for the traffic.
   The IPv4 VIP Type is the only one that has a field for the interface. This is a legacy function from previous versions so that they can be upgraded without complicated reconfigureation. The External IP address, which is a required field, tells the unit which interface to use so it is perfectly acceptable to choose **Any** as the interface. In some configurations, if the Interface field is not set to **Any** the VIP is not one of the displayed options when choosing a destination address.
7. If only specific IP addresses are allowed to be the source address for traffic uing the VIP, check the box for the **Source Address Filter**.

   a. To specific the allowed address range select **Create New.**

   b. Enter the ip address for the start of the set of IP address(es) in the **Range Start** field.

   c. Enter the ip address for the end of the set of IP address(es) in the **Range End** field.
8. Enter the IP address for the **External IP Address/Range**.
   If there is a single IP address, use that address in both fields.
9. Set the **Mapped IP Type**.
   This will be either Subnet or Address Range.
   If you only have a single destination address you can use either:
   - **Subnet**: x.x.x.x/32
   - **Address Range**: x.x.x.x - x.x.x.x, where x.x.x.x is the same IP address.
10. Enter the IP address(es) for the **Mapped IP Address/Range**.
    This will be the address of the host that the traffic is being directed to.
11. If you are only going to use specific ports, enable **Port Forwarding**.

    a. Select one of 3 **Protocol** types:
    - **TCP**
    - **UDP**
    - **SCTP**

b. Enter the port number or range that the traffic will be connecting to in the **External Service Port** fields.

c. Enter the port number or range that is the final destination of the traffic in the **Map to Port** fields

12. Press **OK.**

Example

This example is for a VIP that is being used to direct traffic from the external IP address to a webserver on the internal network.The webserver is for company use only. The company's public facing webserver already used port 80 and there is only one IP external IP address so the traffic for this server is being listened for on port 8080 of the external interface and being sent to port 80 on the internal host.

VIP Type	IPv4
Name	Internal_Webserver
Comments	Webserver with Colaboration tools for Corporate employees
Interface	Any
Source Address Filter	<list of IP addresses of remote users>
External IP Address/Range	172.13.100.27 <this would normally be a public IP address
Mapped IP Type	Subnet
Mapped IP Address/Range	192.168.34.150
Port Forwarding	enabled
Protocol	TCP
External Service Port	8080 - 8080
Map to Port	80 - 80

Virtual IP groups

Just like other address, Virtual IP addresses can be organized into groups for ease of administration. If you have multiple virtual IPs that are likely to be associated to common firewall policies rather than add them individually to each of the policies you can add the instead. That way, if the members of the group change then any changes made to the group will propagate to all of the policies using that group.

When using a Virtual IP address group the firewall policy will take into account all of the configured parameters of the Virtual IPs: IP addresses, Ports and port types.

Creating a virtual IP group

1. Go to **Policy & Objects > Objects > Virtual IPs.**
2. Use the down arrow next to Create New, select **Virtual IP Group**.
3. Select the **Type** fo VIP group you wish to create.
   The options available are:
   a. **IPv4 VIP** - IPv4 on both sides of the FortiGate Unit.
   b. **IPv6 VIP** - IPv6 on both sides of the FortiGate Unit.
   c. **NAT46 VIP** - Going from an IPv4 Network to an IPv6 Network.
   d. **NAT64 VIP** - Going from an IPv6 Network to an IPv4 Network.
   Which is chosen will depend on which of the IP version networks is on the external interface of the FortiGate unit and which is on the internal interface.The options will be:
4. Enter a **Name** for the VIP
5. Enter any additional information in the **Comments** field.
6. Use the dropdown menu of the **Interface** field to select the interface that the member VIPs are associated with, if any.
7. Use the dropdown menu fo the **Members** field to select the VIPs that will be part of the group.
8. Press **OK.**

IP pools

IP pools are a mechanism that allow sessions leaving the FortiGate Firewall to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses will be used instead of the IP address assigned to that FortiGate interface.

When using IP pools for NATing, there is a limitation that must be taken into account. In order for communication to be successful in both directions, it is normal for the source address in the packet header assigned by the NAT process to be an address that is associated with the interface that the traffic is going through. For example, if traffic is going out an interface with the IP address 172.16.100.1, packets would be NATed so that the source IP address would be 172.16.100.1. This way the returning traffic will be directed to the same interface on the same FortiGate that the traffic left from. Even if the packets are assigned a source address that is associated with another interface on the same FortiGate this can cause issues with asymmetrical routing. It is possible to configure the NATed source IP address to be different than the IP address of the interface but you have to make sure that the routing rules of the surrounding network devices take this unorthodox approach into consideration.

There are 4 types of IP Pools that can be configured on the FortiGate firewall:

- One-to-One - in this case the only internal address used by the external address is the internal address that it is mapped to.
- Overload - this is the default setting. Internal addresses other than the one designated in the policy can use this address for the purposes of NAT.
- Fixed Port Range - rather than a single address to be used, there is a range of addresses that can be used as the NAT address. These addresses are randomly assigned as the connections are made.

- Port Block Allocation - this setting is used to allocate a block of port numbers for IP pool users. Two variables will also have to be set. The block size can be set from 64 to 4096 and as the name implies describes the number of ports in one block of port numbers. The number of blocks per user determines how many of these blocks will be assigned. This number can range from 1 to 128.

Be careful when calculating the values of the variables. The maximum number of ports that are available on an address is 65,536. If you chose the maximum value for both variables you will get a number far in excess of the available port numbers.

4096 x 128 = 524,288

One of the more common examples is when you have an email server behind your FortiGate firewall and the range of IP addresses assigned to you by your ISP is more than one. If an organization is assigned multiple IP addresses it is normally considered a best practice to assign a specific address other than the one used for the Firewall to the mail server. However, when normal NAT is used the address assigned to the firewall is also assigned to any outbound sessions. Anti-spam services match the source IP address of mail traffic that they receive to the MX record on DNS servers as an indicator for spam. If there is a mismatch the mail may not get through so there is a need to make sure that the NATed address assigned matches the MX record.

You can also use the Central NAT table as a way to configure IP pools.

Source IP address and IP pool address matching when using a range

When the source addresses are translated to an IP pool that is a range of addresses, one of the following three cases may occur:

Scenario 1:

The number of source addresses equals that of IP pool addresses

In this case, the FortiGate unit always matches the IP addressed one to one.

If you enable fixed port in such a case, the FortiGate unit preserves the original source port. This may cause conflicts if more than one security policy uses the same IP pool, or the same IP addresses are used in more than one IP pool.

Scenario 2:

The number of source addresses is more than that of IP pool addresses

In this case, the FortiGate unit translates IP addresses using a wrap-around mechanism. If you enable fixed port in such a case, the FortiGate unit preserves the original source port. But conflicts may occur since users may have different sessions using the same TCP 5 tuples.

Scenario 3:

The number of source addresses is fewer than that of IP pool addresses

In this case, some of the IP pool addresses are used and the rest of them are not be used.

ARP replies

If a FortiGate firewall interface IP address overlaps with one or more IP pool address ranges, the interface responds to ARP requests for all of the IP addresses in the overlapping IP pools. For example, consider a FortiGate unit with the following IP addresses for the port1 and port2 interfaces:

- port1 IP address: 1.1.1.1/255.255.255.0 (range is 1.1.1.0-1.1.1.255)
- port2 IP address: 2.2.2.2/255.255.255.0 (range is 2.2.2.0-2.2.2.255)

And the following IP pools:

- IP_pool_1: 1.1.1.10-1.1.1.20
- IP_pool_2: 2.2.2.10-2.2.2.20
- IP_pool_3: 2.2.2.30-2.2.2.40

The port1 interface overlap IP range with IP_pool_1 is:

(1.1.1.0-1.1.1.255) and (1.1.1.10-1.1.1.20) = 1.1.1.10-1.1.1.20

The port2 interface overlap IP range with IP_pool_2 is:

(2.2.2.0-2.2.2.255) & (2.2.2.10-2.2.2.20) = 2.2.2.10-2.2.2.20

The port2 interface overlap IP range with IP_pool_3 is:

(2.2.2.0-2.2.2.255) & (2.2.2.30-2.2.2.40) = 2.2.2.30-2.2.2.40

And the result is:

- The port1 interface answers ARP requests for 1.1.1.10-1.1.1.20
- The port2 interface answers ARP requests for 2.2.2.10-2.2.2.20 and for 2.2.2.30-2.2.2.40

Select Enable NAT in a security policy and then select Dynamic IP Pool. Select an IP pool to translate the source address of packets leaving the FortiGate unit to an address randomly selected from the IP pool. Whether or not the external address of an IP Pool will respond to an ARP request can be disabled. You might want to disable the ability to responded to ARP requests so that these address cannot be used as a way into your network or show up on a port scan.

IP pools and zones

Because IP pools are associated with individual interfaces

IP pools cannot be set up for a zone. IP pools are connected to individual interfaces.

Creating a dynamic IP pool

A dynamic IP pool is essintially one in which the IP address that is assigned to the sending computer is not known until the session is created, therefore at the very least it will have to be a pool of at least 2 potential addresses. A quick example would be an IP pool for users of a VPN.

IP Pool Type	IPv4 Pool
Name	Sales_Group_VPN_Users
Comments	<optional>
Type	One-to-One
External IP Range	10.23.0.50 - 10.23.0.75
ARP Reply	[checked]

Fixed port

Some network configurations do not operate correctly if a NAT policy translates the source port of packets used by the connection. NAT translates source ports to keep track of connections for a particular service.

However, enabling the use of a fixed port means that only one connection can be supported through the firewall for this service. To be able to support multiple connections, add an IP pool, and then select Dynamic IP pool in the policy. The firewall randomly selects an IP address from the IP pool and assigns it to each connection. In this case, the number of connections that the firewall can support is limited by the number of IP addresses in the IP pool.

Match-VIP

The match-vip feature allows the FortiGate unit to log virtual IP traffic that gets implicitly dropped. This feature eliminates the need to create two policies for virtual IPs; one that allows the virtual IP, and the other to get proper log entry for DROP rules.

For example, you have a virtual IP security policy and enabled the match-vip feature; the virtual IP traffic that is not matched by the policy is now caught.

The match-vip feature is available only in the CLI. By default, the feature is disabled.

Services and TCP ports

There are a number of different services and protocols in use on the Internet. The most commonly known is HTTP which is used by web servers to transmit requests and responses for unencrypted web pages. These services are set up to listen for requests on a numbered port. These services and protocols can use any port from 1 to 65,535. To keep things simple for everyone a large number of the more commonly used services started using a standardized list of ports. For instance, though it is not required, by default, most web servers listen for HTTP requests on port 80 and by default, web browsers will send HTTP traffic to port 80. If you wish to use another port such as 8080 you would put “:8080” at the end of the URL to indicate that you want the browser to use 8080 instead of the default port.

Example

Default URL for HTTP traffic when the web server is listening on the standard HTTP port:

http://fortinet.com

URL to the same address when the web server is listening for HTTP traffic on port 8080

http://fortinet.com:8080

Services represent typical traffic types and application packets that pass through the FortiGate unit. Firewall services define one or more protocols and port numbers associated with each service. Security policies use service definitions to match session types. You can organize related services into service groups to simplify your security policy list.

Many well-known traffic types have been predefined on the FortiGate unit. If there is a service that does not appear on the list you can create a service or edit an existing one. You need to know the ports, IP addresses or protocols of that particular service or application uses, to create a service.

Best Practices

While you can edit a predefined service it is best to leave those ones alone and create a new service and name it something similar such as the same service name with a descriptive identifier appended.

Based on the previous example, instead of the name “HTTP” you could name the service “HTTP8080” or use the application that is using that port, “HTTP-Application”.

Categories

In order to make sorting through the services easier there is a field to categorize the services. The services can be sorted into the following groups:

- Uncategorized
- General
- Web Access
- File Access
- Email
- Network Services
- Authentication
- Remote Access
- Tunnelling
- VoIP, Messaging and Other Applications
- Web Proxy

To create a new category, use the downward pointing arrow next to **Create New** in the **Services** window and choose **Category**. All that will be required is a name for the new category. A comments describing the new category is optional.

Protocol types

One of the fundamental aspects of a service is the type of protocol that use used to define it. When a service is defined one of the following categories of protocol needs to be determined:

- TCP/UDP/SCTP
- ICMP
- ICMP6
- IP

Depending on which of these protocol categories is choose another set of specifications will can also be defined.

TCP/UDP/SCTP

This is the most commonly used service protocol category. Once this category has been selected the other available options to choose are an address, either IP or FQDN, and the protocol and port number.

The protocol will be TCP, UDP or SCTP.

ICMP or ICMP6

When ICMP or ICMP6 is chosen the available options are the ICMP Type and its code.

IP

When IP is the chosen protocol type the addition option is the Protocol Number.

TCP

Transmission Control Protocol (TCP) is one of the core or fundamental protocols of the Internet. It is part of the Transport Layer of the OSI Model. It is designed to provide reliable delivery of data from a program on one device on the network or Internet to another program on another device on the network or Internet. TCP achieves its reliability because it is a connection based protocol. TCP is stream-oriented. It transports streams of data reliably and in order.

TCP establishes a prior connection link between the hosts before sending data. This is often referred to as the handshake. Once the link is established the protocol uses checks to verify that the data transmitted. If an error check fails the data is retransmitted. This makes sure that the data is getting to the destination error free and in the correct order so that it can be put back together into a form that is identical to the way they were sent.

TCP is configured more for reliability than for speed and because of this TCP will likely be slower than a connectionless protocol such as UDP. This is why TCP is generally not used for real time applications such as voice communication or online gaming.

Some of the applications that use TCP are:

- World Wide Web (HTTP and HTTPS)
- Email (SMTP, POP3, IMAP4)
- Remote administration (RDP)
- File transfer (FTP)

UDP

User Datagram Protocol (UDP) like TCP is one of the core protocols of the Internet and part of the Transport Layer of the OSI Model. UDP is designed more for speed than reliability and is generally used for different applications than TCP. UDP sends messages, referred to as datagrams across the network or Internet to other hosts without establishing a prior communication link. In other words, there is no handshake.

UDP is an unreliable service as the datagrams can arrive out of order, duplicated or go missing without any mechanism to verify them. UDP works on the assumption that any error checking is done by the application or is not necessary for the function of the application. This way it avoids the overhead that is required to verify the integrity of the data.

This lack of overhead improves the speed of the data transfer and is why UDP is often used by applications that are time sensitive in nature. UDP's stateless nature is also great for applications that answer a large number of small queries from a large number of clients.

Common uses for UDP are:

- Domain Name Resolution (DNS)
- Time (NTP)
- Streaming media (RTSP, RTP and RTCP)
- Telephone of the Internet (VoIP)
- File Transfer (TFTP)
- Logging (SNMP)
- Online games (GTP and OGP)

SCTP

Stream Control Transmission Protocol (SCTP) is part of the Transport Layer of the OSI Model just like TCP and UDP and provides some of the features of both of those protocols. It is message or datagram orientated like UDP but it also ensures reliable sequential transport of data with congestion control like TCP.

SCTP provides the following services:

- Acknowledged error-free non-duplicated transfer of user data
- Data fragmentation to conform to discovered path MTU size
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages
- Optional bundling of multiple user messages into a single SCTP packet
- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association
- Congestion avoidance behavior and resistance to flooding and masquerade attacks

SCTP uses multi-streaming to transport its messages which means that there can be several independent streams of messages traveling in parallel between the points of the transmission. The data is sent out in larger chunks of data than is used by TCP just like UDP but the messages include a sequence number within each message in the same way that TCP does so that the data can be reassembled at the other end of the transmission in the correct sequence without the data having to arrive in the correct sequence.

SCTP is effective as the transport protocol for applications that require monitoring and session-loss detection. For such applications, the SCTP path and session failure detection mechanisms actively monitor the connectivity of the session. SCTP differs from TCP in having multi-homing capabilities at either or both ends and several streams within a connection, typically referred to as an association. A TCP stream represents a sequence of bytes; an SCTP stream represents a sequence of messages.

Some common applications of SCTP include supporting transmission of the following protocols over IP networks:

- SCTP is important in 3G and 4G/LTE networks (for example, HomeNodeB = FemtoCells)
- SS7 over IP (for example, for 3G mobile networks)
- SCTP is also defined and used for SIP over SCTP and H.248 over SCTP
- Transport of Public Switched Telephone Network (PSTN) signaling messages over IP networks.

SCTP is a much newer protocol. It was defined by the IETF Signaling Transport (SIGTRAN) working group in 2000. It was introduced by RFC 3286 and more fully define by RFC 4960.

The FortiGate firewall can apply security policies to SCTP sessions in the same way as TCP and UDP sessions. You can create security policies that accept or deny SCTP traffic by setting the service to “ALL”. FortiOS does not include pre-defined SCTP services. To configure security policies for traffic with specific SCTP source or destination ports you must create custom firewall services for SCTP.

FortiGate units route SCTP traffic in the same way as TCP and UDP traffic. You can configure policy routes specifically for routing SCTP traffic by setting the protocol number to 132. SCTP policy routes can route SCTP traffic according to the destination port of the traffic if you add a port range to the policy route.

You can configure a FortiGate unit to perform stateful inspection of different types of SCTP traffic by creating custom SCTP services and defining the port numbers or port ranges used by those services. FortiGate units support SCTP over IPv4. The FortiGate unit performs the following checks on SCTP packets:

- Source and Destination Port and Verification Tag.
- Chunk Type, Chunk Flags and Chunk Length
- Verify that association exists
- Sequence of Chunk Types (INIT, INIT ACK, etc)
- Timer checking
- Four way handshake checking
- Heartbeat mechanism
- Protection against INIT/ACK flood DoS attacks, and long-INIT flooding
- Protection against association hijacking

FortiOS also supports SCTP sessions over IPsec VPN tunnels, as well as full traffic and event logging for SCTP sessions.

Specific addresses in TCP/UDP/SCTP

In the TCP/UDP/SCTP services it is also possible to set the parameter for a specific IP or Fully Qualified Domain Name address. The IP/FQDN field refers to the destination address of the traffic, not the source. This means for example, that you can set up a custom service that will describe in a policy the TCP traffic over port 80 going to the web site example.com, but you cannot set up a service that describes the TCP traffic over port 80 that is coming from the computer with the address 192.168.29.59.

Protocol port values

The source and destination ports for TCP/UDP/SCTP services are important to get correct. If they are reversed the service will not work. The destination port(s) are the on ones that refer to the ports that the computer will be listening on. These are the port numbers that most people are familiar with when they associate a port number to a protocol. In most cases the source port will be one that is randomly assigned by the computer that is not being already used by another service.

Most people associate HTTP with port 80. This means that a web-server will be listening on port 80 for any http requests being sent to the computer. The computer that is sending the request can use any port that is not already assigned to another service or communication session. There are 65,535 ports that it can randomly assign, but because the ports from 1 to 1024 are normally used for listening for incoming communications it is usually not in that range. It is unless there is a specific instance when you know that a communication will be coming from a predefined source port it is best practice to set the source port range from 1 to 65,535.

ICMP

The Internet Control Message Protocol (ICMP) is a protocol layered onto the Internet Protocol Suite to provide error reporting flow control and first-hop gateway redirection. It is normally used by the operating systems of networked computers to send connectivity status query, response and error messages. It is assigned protocol number 1. There is a version of the protocol for both IPv4 and for IPv6. It is not designed to be absolutely reliable like TCP.

ICMP is not typically used for transporting data or for end-user network applications with the exception of some diagnostic utilities such as ping and traceroute.

ICMP messages are sent in several situations, for example:

- when a datagram cannot reach its destination,
- time exceeded messages
- redirect messages
- when the gateway does not have the buffering capacity to forward a datagram
- when the gateway can direct the host to send traffic on a shorter route.

Some of the specific ICMP message types are:

- ICMP_ECHO
- ICMP_TIMESTAMP
- ICMP_INFO_REQUEST
- ICMP_ADDRESS

For ICMP error messages, only those reporting an error for an existing session can pass through the firewall. The security policy will allow traffic to be routed, forwarded or denied. If allowed, the ICMP packets will start a new session. Only ICMP error messages of a corresponding security policy is available will be sent back to the source. Otherwise, the packet is dropped. That is, only ICMP packets for a corresponding security policy can traverse the FortiGate unit.

ICMP types and codes

ICMP has a number of messages that are identified by the “Type” field. Some of these types have assigned “Code” fields as well. The table below shows the different types of ICMP Types with their associated codes if there are any.

ICMP types and codes

Type Number	Type Name	Optional Code(s)
0	Echo Reply	
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	0 Net Unreachable 1 Host Unreachable 2 Protocol Unreachable 3 Port Unreachable 4 Fragmentation Needed and Don't Fragment was Set 5 Source Route Failed 6 Destination Network Unknown 7 Destination Host Unknown 8 Source Host Isolated 9 Communication with Destination Network is Administratively Prohibited 10 Communication with Destination Host is Administratively Prohibited 11 Destination Network Unreachable for Type of Service 12 Destination Host Unreachable for Type of Service 13 Communication Administratively Prohibited 14 Host Precedence Violation 15 Precedence cutoff in effect
4	Source Quench	
5	Redirect	0 Redirect Datagram for the Network (or subnet) 1 Redirect Datagram for the Host 2 Redirect Datagram for the Type of Service and Network 3 Redirect Datagram for the Type of Service and Host

Type Number	Type Name	Optional Code(s)
6	Alternate Host Address	
7	Unassigned	
8	Echo	
9	Router Advert-isement	
10	Router Selection	
11	Time Exceeded	0 Time to Live exceeded in Transit 1 Fragment Reassembly Time Exceeded
12	Parameter Problem	0 Pointer indicates the error 1 Missing a Required Option 2 Bad Length
13	Timestamp	
14	Timestand Reply	
15	Information Request	
16	Information Reply	
17	Address Mask Request	
18	Address Mask Reply	
19	Reserved (for Security)	
20 - 29	Reserved (for Robustness Exper-iment)	
30	Traceroute	
31	Datagram Con-version Error	

Type Number	Type Name	Optional Code(s)
32	Mobile Host Redirect	
33	IPv6 Where-Are-You	
34	IPv6 I-Am-Here	
35	Mobile Registration	
36	Mobile Registration Reply	
37	Domain Name Request	
38	Domain Name Reply	
39	SKIP	
40	Photuris	
41 - 255	Reserved	

log-invalid-packet

The `log-invalid-packet` CLI setting is one that is intended to log invalid ICMP packets. The exact definition being:

> If the ForitGate unit receives an ICMP error packet that contains an embedded `IP(A,B)|TCP (C,D)` header, then if FortiOS can loacate the A:C -> B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped.

When this field is enabled, the FortiGate also log messages that are not ICMP error packets.

Types of logs covered by `log-invalid-packet`

- Invalid ICMP
  - If ICMP error message verification (see "check-reset-range") is enabled
- Invalid DNS packets
  - DNS packets that contain requests for non-existing domains
- `iprope` check failed
- reverse path check fail
- denied and broadcast traffic
- no session matched

Some other examples of messages that are not errors that will be logged, based on RFC792:

Type 3 messages correspond to "Destination Unreachable Message"

- Type 3, Code 1 = host unreachable
- Type 3, Code 3 = port unreachable

Type 11 messages correspond to "Time Exceeded Message"

- Type 11, Code 0 = time to live exceeded in transit

ICMPv6

Internet Control Message Protocol version 6 (ICMPv6) is the new implementation of the Internet Control Message Protocol (ICMP) that is part of Internet Protocol version 6 (IPv6). The ICMPv6 protocol is defined in RFC 4443.

ICMPv6 is a multipurpose protocol. It performs such things as:

- error reporting in packet processing
- diagnostic functions
- Neighbor Discovery process
- IPv6 multicast membership reporting

It also designed as a framework to use extensions for use with future implementations and changes.

Examples of extensions that have already been written for ICMPv6:

- Neighbor Discovery Protocol (NDP) - a node discovery protocol in IPv6 which replaces and enhances functions of ARP.
- Secure Neighbor Discovery Protocol (SEND) - an extension of NDP with extra security.
- Multicast Router Discovery (MRD) - allows discovery of multicast routers.

ICMPv6 messages use IPv6 packets for transportation and can include IPv6 extension headers. ICMPv6 includes some of the functionality that in IPv4 was distributed among protocols such as ICMPv4, ARP (Address Resolution Protocol), and IGMP (Internet Group Membership Protocol version 3).

ICMPv6 has simplified the communication process by eliminating obsolete messages.

ICMPv6 messages are subdivided into two classes: error messages and information messages.

Error Messages are divided into four categories:

1. Destination Unreachable
2. Time Exceeded
3. Packet Too Big
4. Parameter Problems

Information messages are divided into three groups:

1. Diagnostic messages
2. Neighbor Discovery messages
3. Messages for the management of multicast groups.

ICMPv6 types and codes

ICMPv6 has a number of messages that are identified by the “Type” field. Some of these types have assigned “Code” fields as well. The table below shows the different types of ICMP Types with their associated codes if

there are any.

Type codes 0 − 127 are error messages and type codes 128 − 255 are for information messages.

ICMPv6 Types and Codes

Type Number	Type Name	Code
0	Reserved	0 - no route to destination 1 - communication with destination administratively prohibited 2 - beyond scope of source address 3 - address unreachable 4 - port unreachable 5 - source address failed ingress/egress policy 6 - reject route to destination 7 - Error in Source Routing Header
1	Destination Unreachable	
2	Packet Too Big	
3	Time Exceeded	0 - hop limit exceeded in transit 1 - fragment reassembly time exceeded
4	Parameter Problem	0 - erroneous header field encountered 1 - unrecognized Next Header type encountered 2 - unrecognized IPv6 option encountered
100	Private Exper-imentation	
101	Private Exper-imentation	
102 - 126	Unassigned	
127	Reserved for expan-sion if ICMPv6 error messages	
128	Echo Request	
129	Echo Replay	

Type Number	Type Name	Code
130	Multicast Listener Query	
131	Multicast Listener Report	
132	Multicast Listener Done	
133	Router Solicitation	
134	Router Advert-isement	
135	Neighbor Soli-citation	
136	Neighbor Advert-isement	
137	Redirect Message	
138	Router Renum-bering	0 - Router Renumbering Command 1 - Router Renumbering Result 255 - Sequence Number Reset
139	ICMP Node Inform-ation Query	0 - The Data field contains an IPv6 address which is the Subject of this Query. 1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP. 2 - The Data field contains an IPv4 address which is the Subject of this Query.
140	ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty. 1 - The Responder refuses to supply the answer. The Reply Data field will be empty. 2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.

Type Number	Type Name	Code
141	Inverse Neighbor Discovery Solicitation Message	
142	Inverse Neighbor Discovery Advertisement Message	
143	Version 2 Multicast Listener Report	
144	Home Agent Address Discovery Request Message	
145	Home Agent Address Discovery Reply Message	
146	Mobile Prefix Solicitation	
147	Mobile Prefix Advertisement	
148	Certification Path Solicitation Message	
149	Certification Path Advertisement Message	
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	
151	Multicast Router Advertisement	
152	Multicast Router Solicitation	
153	Multicast Router Termination	

Type Number	Type Name	Code
154	FMIPv6 Messages	
155	RPL Control Message	
156	ILNPv6 Locator Update Message	
157	Duplicate Address Request	
158	Duplicate Address Confirmation	
159 – 199	Unassigned	
200	Private experimentation	
201	Private experimentation	
255	Reserved for expansion of ICMPv6 informational messages	

IP

Internet Protocol (IP) is the primary part of the Network Layer of the OSI Model that is responsible for routing traffic across network boundaries. It is the protocol that is responsible for addressing. IPv4 is probable the version that most people are familiar with and it has been around since 1974. IPv6 is its current successor and due to a shortage of available IPv4 addresses compared to the explosive increase in the number of devices that use IP addresses, IPv6 is rapidly increasing in use.

When IP is chosen as the protocol type the available option to further specify the protocol is the protocol number. This is used to narrow down which protocol within the Internet Protocol Suite and provide a more granular control.

Protocol number

IP is responsible for more than the address that it is most commonly associated with and there are a number of associated protocols that make up the Network Layer. While there are not 256 of them, the field that identifies them is a numeric value between 0 and 256.

In the Internet Protocol version 4 (IPv4) [RFC791] there is a field called “Protocol” to identify the next level protocol. This is an 8 bit field. In Internet Protocol version 6 (IPv6) [RFC2460], this field is called the “Next Header” field.

Protocol Numbers

#	Protocol	Protocol's Full Name
0	HOPOPT	IPv6 Hop-by-Hop Option
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IPv4	IPv4 encapsulation Protocol
5	ST	Stream
6	TCP	Transmission Control Protocol
7	CBT	CBT
8	EGP	Exterior Gateway Protocol
9	IGP	Any private interior gateway (used by Cisco for their IGRP)
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram Protocol
18	MUX	Multiplexing
19	DCN-MEAS	DCN Measurement Subsystems
20	HMP	Host Monitoring
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
23	TRUNK-1	Trunk-1

#	Protocol	Protocol's Full Name
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Protocol Class 4
30	NETBLT	Bulk Data Transfer Protocol
31	MFE-NSP	MFE Network Services Protocol
32	MERIT-INP	MERIT Internodal Protocol
33	DCCP	Datagram Congestion Control Protocol
34	3PC	Third Party Connect Protocol
35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	XTP
37	DDP	Datagram Delivery Protocol
38	IDPR-CMTP	IDPR Control Message Transport Proto
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41	IPv6	IPv6 encapsulation
42	IPv6	SDRPSource Demand Routing Protocol
43	IPv6-Route	Routing Header for IPv6
44	IPv6-Frag	Fragment Header for IPv6
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Reservation Protocol
47	GRE	General Routing Encapsulation

#	Protocol	Protocol's Full Name
48	DSR	Dynamic Source Routing Protocol
49	BNA	BNA
50	ESP	Encap Security Payload
51	AH	Authentication Header
52	I-NLSP	Integrated Net Layer Security TUBA
53	SWIPE	IP with Encryption
54	NARP	NBMA Address Resolution Protocol
55	MOBILE	IP Mobility
56	TLSP	Transport Layer Security Protocol using Kryptonet key management
57	SKIP	SKIP
58	IPv6-ICMP	ICMP for IPv6
59	IPv6-NoNxt	No Next Header for IPv6
60	IPv6-Opts	Destination Options for IPv6
61		any host internal protocol
62	CFTP	CFTP
63		any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
67	IPPC	Internet Pluribus Packet Core
68		any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
71	IPCV	Internet Packet Core Utility

#	Protocol	Protocol's Full Name
72	CPNX	Computer Protocol Network Executive
73	CPHB	Computer Protocol Heart Beat
74	WSN	Wang Span Network
75	PVP	Packet Video Protocol
76	BR-SAT-MON	Backroom SATNET Monitoring
77	SUN-ND	SUN ND PROTOCOL-Temporary
78	WB-MON	WIDEBAND Monitoring
79	WB-EXPAK	WIDEBAND EXPAK
80	ISO-IP	ISO Internet Protocol
81	VMTP	VMTP
82	SECURE-VMTP	SECURE-VMTP
83	VINES	VINES
84	TTP	TTP
84	IPTM	Protocol Internet Protocol Traffic
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	EIGRP	EIGRP
89	OSPFIGP	OSPFIGP
90	Sprite-RPC	Sprite RPC Protocol
91	LARP	Locus Address Resolution Protocol
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25 Frames
94	IPIP	IP-within-IP Encapsulation Protocol

#	Protocol	Protocol's Full Name
95	MICP	Mobile Internetworking Control Pro.
96	SCC-SP	Semaphore Communications Sec. Pro.
97	ETHERIP	Ethernet-within-IP Encapsulation
98	ENCAP	Encapsulation Header
99		any private encryption scheme
100	GMTP	GMTP
101	IFMP	Ipsilon Flow Management Protocol
102	PNNI	PNNI over IP
103	PIM	Protocol Independent Multicast
104	ARIS	ARIS
105	SCPS	SCPS
106	QNX	QNX
107	A/N	Active Networks
108	IPComp	IP Payload Compression Protocol
109	SNP	Sitara Networks Protocol
110	Compaq-Peer	Compaq Peer Protocol
111	IPX-in-IP	IPX in IP
112	VRRP	Virtual Router Redundancy Protocol
113	PGM	PGM Reliable Transport Protocol
114		any 0-hop protocol
115	L2TP	Layer Two Tunneling Protocol
116	DDX	D-II Data Exchange (DDX)
117	IATP	Interactive Agent Transfer Protocol
118	STP	Schedule Transfer Protocol

#	Protocol	Protocol's Full Name
119	SRP	SpectraLink Radio Protocol
120	UTI	UTI
121	SMP	Simple Message Protocol
122	SM	SM
123	PTP	Performance Transparency Protocol
124	ISIS over IPv4	
125	FIRE	
126	CRTP	Combat Radio Transport Protocol
127	CRUDP	Combat Radio User Datagram
128	SSCOPMCE	
129	IPLT	
130	SPS	Secure Packet Shield
131	PIPE	Private IP Encapsulation within IP
132	SCTP	Stream Control Transmission Protocol
133	FC	Fibre Channel
134	RSVP-E2E-IGNORE	
135	Mobility Header	
136	UDPLite	
137	MPLS-in-IP	
138	manet	
139	HIP	
140	Shim6	
141	WESP	
142	ROHC	

#	Protocol	Protocol's Full Name
143 – 252	Unassigned	Unassigned
253		Use for experimentation and testing
254		Use for experimentation and testing
255	Reserved	

Further information can be found by researching RFC 5237.

Service groups

Just like some of the other firewall components, services can also be bundled into groups for ease of administration.

Creating a service group

1. Go to **Policy & Objects > Objects > Services**.
2. Select the down arrow next to **Create New**, select **Service Group**.
3. Input a Group Name for the list of services.
4. Input any additional information in the Comments field.
5. Choose a **Type**; either **Firewall** or **Explicit Proxy**.
6. Next to Members there is a dropdown menu that can be used to select from the available Services. It is possible to select more than 1 entry. Just select the green plus sign next to the field to add an additional entry. Select the “X” icon in the field to remove an entry.
7. Press **OK**.

Example scenario: Supporting audio/visual conferencing

The feature, and the transmitting of data for the purpose of, Tele-conferencing or Audio/Visual Conferencing is covered by a number of standards:

- The IETF standard known as the Binary Floor Control Protocol (BFCP).
- RFC 4582, for SIP-based video devices
- The ITU standard H.239 (for H.323-based video devices)

While these standards have been set up by various authoritative bodies and can take place on different layers of the OSI model, they share common requirements that are addressed by the FortiGate firewall’s ability to manage the traffic and the protocols involved. This means that the same ability that make the device RFC 4582 compliant makes it compliant with H.239 as well.

To demonstrate how services and service groups are used we show the setup of a firewall that will need to support the connectivity of a video conferencing unit. The FortiGate does not manipulate or change the content of the traffic but it does allow for the traffic to pass through the device. In this case it allow for only the needed

traffic to pass through the device so as to allow the functionality of Audio Visual Conference call but not to allow other traffic through.

The theoretical location for this scenario is a hospital that hosts conferences and lectures from doctors from all over the world, sometimes from multiple locations, using video conferencing technology such as a Polycom Video Conference system. There is a special room set up with dedicated Ethernet connectivity to the Internet. A hospital has a lot of sensitive information going over its network so the setup has to be secure to prevent any chance of penetration.

The approach is fairly simple. The conference room has a dedicated port on the FortiGate (port #7) and its own LAN. We will assume that the interface has already been configured properly. Video conference traffic can come from the Internet to the Polycom in that room and traffic can get out to the Internet, but traffic going to other areas of the hospital network have to go through the FortiGate and traffic going from the Video Conference LAN is thoroughly filtered.

To give an idea of how extensive this can be, we will use an extreme case and include just about all of the services that could be commonly used in one of these setups. The protocols listed here may differ from other setups. It will depend on which features are being used and which equipment is within the network. Always check the documentation that comes with the set up before opening ports into your network.

VIP

In this particular case there is an IP address set aside for the conferencing system so a separate VIP is not needed for every port. One Virtual IP will be created for the system and then only the approved of protocols will be allows through the firewall.

Name	Vid-Conf_Room216
External Interface	wan1
External IP Address/Range	256.87.212.51 – 256.87.212.51
Mapped IP Address/Range	192.168.7.25 – 192.168.7.25
Port Forwarding	not selected

Creating an address for the subnet

In the same way that the VIP was created to identify and direct incoming traffic an address should be created to identify the addresses of computer that will be in the Conference room. This included computers on the LAN as well as the Teleconferencing equipment.

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**.
3. Fill out the fields with the following information:

Category	Address

Name	Port7_subnet
Type	Subnet
Subnet/IP Range	192.168.7.0/255.255.255.0
Interface	port7
Show in address list	checked

Configuring the services

Services already created:

The following are standard services that have already been created by default:

HTTP	TCP 80
SNMP	TCP 161-162/UDP 161-162
LDAP	TCP 389
HTTPS	TCP 443
SYSLOG	UDP 514

Existing services to be edited:

There are a few services that have already been created for you, but they need to be expanded to accommodate the list of protocols listed for this scenario.

The default h323 contains:

- TCP 1503
- UDP 1719
- TCP 1720

We need to add:

- TCP1719

The default SIP contains:

- UDP 5060

We need to add:

- TCP 5060

H323 service

1. Go to **Policy & Objects > Objects > Services**.
2. Scroll down to the section: **VoIP, Messaging & Other Applications**.
3. Select **H323**.
4. Select **Edit**.
5. In the Protocol section add the additional protocol:

Protocol Type	TCP
Destination port /Low	1719

6. Select **OK** to save.

SIP service

1. Go to **Policy & Objects > Objects > Services**.
2. Scroll down to the section: **VoIP, Messaging & Other Applications**.
3. Select **SIP**.
4. Select **Edit**.
5. In the Protocol section add the additional protocol:

Protocol Type	TCP
Destination port /Low	5060

6. Select **OK** to save.

Custom services that need to be created

There are a number of possible services that may need to be added from scratch rather than editing existing ones. While it is possible to create a single custom service that contains all of the open ports needed, it make more sense to make this modular in case only a small subset of the service needs to be added to another policy.

Polycom API

1. Go to **Policy & Objects > Objects > Services**.
2. Select **Create New**.
3. Fill in the fields of the new service with the following information:

Name	Polycom API
Service Type	Firewall
Category	VoIP, Messaging & Other
Protocol Type	TCP/UDP/SCTP

Protocol	TCP/UDP/SCTP
Protocol	TCP
Destination Port - Low:	24
Destination Port - High:	<leave blank>

4. Select **OK**.

Polycom endpoints

1. Go to **Policy & Objects > Objects > Services**.
2. Select **Create New**.
3. Fill in the fields of the new service with the following information:

Name	Polycom Endpoints
Service Type	Firewall
Category	VoIP, Messaging & Other
Protocol Type	TCP/UDP/SCTP
Protocol	TCP
Destination - Low:	3230
Destination - High:	3253

4. Select **OK**.

Other Services to add in the same way:

Name of Service	Category	Protocol & Port #
LDAP secure communications	Authentication	TCP 636
Win 2000 ILS Registration	Network Services	TCP 1002
Gatekeeper discovery	VoIP, Messaging & Other Applications	TCP 1718
Audio Call Control	VoIP, Messaging & Other Applications	TCP 1731
Polycom proprietary Global directory data	VoIP, Messaging & Other Applications	TCP 3601
Polycom People+Content	VoIP, Messaging & Other Applications	TCP 5001
HTTP Server Push	Web Access	

Creating the service group

1. Go to **Firewall Objects > Service > Groups**.
2. Select **Create New**.
3. Build the Service group by filing in the fields with the following information

Group Name	A-V_Conference
Type	Firewall
Members (click in the drop down menu to add the following services)	• HTTP • SNMP • LDAP • HTTPS • SYSLOG • Polycom API • Polycom Endpoints • LDAP secure communications • Win 2000 ILS Registration • Gatekeeper discovery • Audio Call Control • Polycom proprietary Global directory data • Polycom People+Content • HTTP Server Push

Creating the IPS security profile

This is by no means the only way to set up this IPS filter, but it is the way that the fictional System Administrator wants it set up. Yours may be different.

1. Go to Security **Profiles > Intrusion Protection > IPS Sensors**.
2. Create a new sensor.

Name	A-V_Conference-incoming

3. Select **OK.**
4. In the newly created sensor, create a new IPS filter.

Sensor Type	Filter Based
Filter Options	Advanced
Severity	• Critical • High • Medium • Low
Target	Server
OS	Windows

Application	• IIS • other
Protocol **Use the [Show more...] option**	• HTTP • LDAP • SIP • SSL • H323
Packet logging	enabled

Based on these filters there should be somewhere in the neighborhood of 750 signatures that the FortiGate will run traffic against in the IPS engine.

Policies

Incoming policy

A policy has to be made to allow the traffic to come in from the Internet to connect to the Tele-conferencing server equipment.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Fill out the fields with the following information:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	wan1
Source Address	all
Outgoing Interface	port7
Destination Address	Vid-Conf_Room216
Schedule	always
Service	A-V_Conference
Action	ACCEPT
Enable NAT	<not enabled>
Logging Options	Logging is a good idea but how much will depend on storage capabilities.
Security Profiles	Turn on IPS and choose “A-V_Conference-incoming”
Traffic Shaping, Web cache, WAN Optimization, Disclaimer:	The use of these features will depend on your network environment and should be decided by the network architect, as the decision will largely be based on network bandwidth, usage and importance of Video conferencing compared to other traffic.

4. Select **OK**.

The policy will then need to be put in the correct position in the sequence of the policies. Because it is a rather focused policy it should be acceptable to place it near the top of the policy order sequence.

Outgoing policy

A policy has to be made to allow the traffic to leave from the subnet in the conference room to the Internet, not only for the traffic for the Tele-conferencing equipment but for normal traffic of users on the Internet such as web research and email. The traffic is outgoing so there is less of a need for an Intrusion Protection System filter, but check with the network architect in case there is a need for using one of the other security profiles.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Fill out the fields with the following information:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	port7
Source Address	Port7_subnet
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	any
Action	ACCEPT
Enable NAT	enabled Use Destination Interface Address
Logging Options	Logging is a good idea but how much will depend on storage capabilities.
Security Profiles	<see above>
Traffic Shaping, Web cache, WAN Optimization, Disclaimer:	The use of these features will depend on your network environment and should be decided by the network architect, as the decision will largely be based on network bandwidth, usage and importance of Video conferencing compared to other traffic.

4. Select **OK**.

The policy will then need to be put in the correct position in the sequence of the policies.

Firewall schedules

Firewall schedules control when policies are in effect. When you add a security policy on a FortiGate unit you need to set a schedule to determine the time frame in which that the policy will be functioning. While it is not set by default, the normal schedule would be always. This would mean that the policy that has been created is

always function and always policing the traffic going through the FortiGate. The time component of the schedule is based on a 24 hour clock notation or military time as some people would say.

There are two types of schedules: One-time schedules and recurring schedules.

One-Time schedules are in effect only once for the period of time specified in the schedule. This can be useful for testing to limit how long a policy will be in effect in case it is not removed, or it can be used for isolated events such as a conference where you will only need a temporary infrastructure change for a few days.

The time frame for a One-time schedule is configured by using a start time which includes, Year | Month | Day | Hour | Minute and a Stop time which includes the same variables. So while the frequency of the schedule is only once it can last anywhere from 1 minute to multiple years.

Recurring schedules are in effect repeatedly at specified times of specified days of the week. The Recurring schedule is based on a repeating cycle of the days of the week as opposed to every x days or days of the month. This means that you can configure the schedule to be in effect on Tuesday, Thursday, and Saturday but not every 2 days or on odd numbered days of the month.

If a recurring schedule has a stop time that is earlier than the start time, the schedule will take effect at the start time but end at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next.

> Because recurring schedules do not work with DENY policies, the strategy when designing a schedule should *not* be to determine when users cannot access a policy but to build the schedules around when it *is* possible to access the policy.

Example

You want to schedule the use of Skype to only between noon (12:00) and 1 p.m. (13:00).

You could create a schedule that allows Skype traffic:

- Starting at Hour:12 and Minute: 00
- Stopping at Hour:13 and Minute: 00
- Set for days of the week: Sunday | Monday |Tuesday |Wednesday | Thursday | Friday | Saturday

Or you could have a schedule that blocks Skype traffic:

- Starting at Hour:13 and Minute: 00 (and goes to the next day)
- Stopping at Hour:12 and Minute: 00
- Set for days of the week: Sunday | Monday |Tuesday |Wednesday | Thursday | Friday | Saturday

Either way is effective for the task but other factors may make one method work better than another in certain situations of it could be just a preference in approach.

Schedule expiration

The schedule in a security policy enables certain aspects of network traffic to occur for a specific length of time. What it does not do however, is police that time. That is, the policy is active for a given time frame, and as long as the session is open, traffic can continue to flow.

For example, in an office environment, Skype use is allowed between noon and 1pm. During that hour, any Skype traffic continues. As long as that session is open, after the 1pm end time, the Skype conversations can continue, yet new sessions will be blocked. Ideally, the Skype session should close at 1pm.

Using a CLI command you can set the schedule to terminate all sessions when the end time of the schedule is reached. Within the config firewall command enter the command:

```
set schedule-timeout enable
```

By default, this option is set to disable.

A few further settings are needed to make this work.

```
config firewall policy
   edit ID
      set firewall-session-dirty check-new
      end

config system settings
   set firewall-session-dirty check-policy-option
      end
```

Firewall-session-dirty setting

The firewall-session-dirty setting has three options

`check-all`	CPU flushes all current sessions and re-evaluates them. [default]
`check-new`	CPU keeps existing sessions and applies policy changes to new sessions only. This reduces CPU load and the possibility of packet loss.
`check-policy-option`	Use the option selected in the firewall-session-dirty field of the firewall policy (check-all or check-new, as above, but per policy).

Schedule groups

You can organize multiple firewall schedules into a schedule group to simplify your security policy list. The schedule parameter in the policy configuration does not allow for the entering of multiple schedules into a single policy so if you have a combination of time frames that you want to schedule the policy for then the best approach, rather than making multiple policies is to use a schedule group.

Example

Your Internet policy allows employees to visit Social Media sites from company computers but not during what is considered working hours. The offices are open a few hours before working hours and the doors are not locked until a few hours after official closing so work hours are from 9 to 5 with a lunch break from Noon to 1:00 p.m.

Your approach is to block the traffic between 9 and noon and between 1:00 p.m. and 5:00 p.m. This means you will need two schedules for a single policy and the schedule group handles this for you. Schedule groups can contain both recurring and one-time schedules. Schedule groups cannot contain other schedule groups.

Schedule expiration

The schedule in a security policy enables certain aspects of network traffic to occur for a specific length of time. What it does not do however, is police that time. That is, the policy is active for a given time frame, and as long as

the session is open, traffic can continue to flow.

For example, in an office environment, Skype use is allowed between noon and 1pm. During that hour, any Skype traffic continues. As long as that session is open, after the 1pm end time, the Skype conversations can continue, yet new sessions will be blocked. Ideally, the Skype session should close at 1pm.

Using a CLI command you can set the schedule to terminate all sessions when the end time of the schedule is reached. Within the config firewall command enter the command:

```
set schedule-timeout enable
```

By default, this is set to `disable`.

Security policies

One of the foundations upon which a firewall works is the use of policies. These are what bring the other firewall objects and components together into an elegant mechanism for the governing of the traffic going through the network.

This Chapter includes information on the following topics:

- Firewall policies
- Security profiles
- SSL/SSH Inspection
- Identity Based Policies
- Device Identity Policies
- VPN Policies
- Interface Policies
- One-Arm IDS
- Local-In Policies
- Security Policy 0
- Deny Policies
- Accept Policies
- IPv6 Policies
- Fixed Port
- Endpoint Security
- Traffic Logging
- Quality of Service
- Policy Monitor

Firewall policies

The firewall policy is the axis around which most of the other features of the FortiGate firewall revolve. A large portion of the settings in the firewall at some point will end up relating to or being associated with the firewall policies and the traffic that they govern. Any traffic going through a FortiGate unit has to be associated with a policy. These policies are essentially discrete compartmentalized sets of instructions that control the traffic flow going through the firewall. These instructions control where the traffic goes, how it's processed, if it's processed and even whether or not it's allowed to pass through the FortiGate.

When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it will need to use and the time of day. Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed.

The 2 basic actions at the initial connection are either ACCEPT or DENY:

- If the Action is ACCEPT, the policy action permits communication sessions. There may be other packet processing instructions, such as requiring authentication to use the policy. While you may not see it in the configuration there is the implied subset of the ACCEPT Action that include VPN policies, whether they be an IPsec VPN or SSL.
- If the Action is DENY, the policy action blocks communication sessions, and you can optionally log the denied traffic. If no security policy matches the traffic, the packets are dropped. A DENY security policy is needed when it is required to log the denied traffic, also called “violation traffic”.

The policy may contain a number of instructions for the FortiGate firewall in addition to the ACCEPT or DENY actions, some of which are optional. Instructions on how to process the traffic can also include such things as:

- Logging Traffic
- Authentication
- Network Address Translation or Port Address Translation
- Use Virtual IPs or IP Pools
- Caching
- Whether to use address or Identity based rules
- Whether to treat as regular traffic or VPN traffic
- What certificates to use
- Security profiles to apply
- Proxy Options
- Traffic Shaping

Firewall policy parameters

As mentioned before, for traffic to flow through the FortiGate firewall there must be a policy that matches its parameters:

Incoming interface

This is the interface or interfaces that the traffic is first connection to the FortiGate unit by. The exception being traffic that the FortiGate generates itself. This is not limited to the physical Ethernet ports found on the device. The incoming interface can also be a logical or virtual interface such as a VPN tunnel, a Virtual WAN link or a wireless interface.

Outgoing interface

After the firewall has processed the traffic it needs to leave a port to get to its destination and this will be the interface or interfaces that the traffic leaves by. This interface, like the **Incoming Interface** is not limited to only physical interfaces.

Source address

The addresses that a policy can receive traffic from can be wide open or tightly controlled. For a public webserver that the world at large should be able to access, the best choice will be “all”. If the destination is a private webserver that only the branch offices of a company should be able to access or a list of internal computers that are the only ones allowed to access an external resource then a group of preconfigured addresses is the better strategy.

Additional parameters under the Source Address, though they are not manditory are:

- **Source User(s)**
  This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group that has been set up in advance that can be sellected from the dropdown menu. The exception to this is the feature that allows the importing of LDAP Users. When the feature is used, a small wizard window will appear to guide the user through the setup. The caveat is that the LDAP server object in the **User and Device > Authentication > LDAP Servers** section has to be already configured to allow the use of this import feature.
- **Source Device Type**
  This parameter is for narrowing down the traffic sending devices to those that the FortiGate is familiar with. Again the the contents of this parameter need to be a preconfigured object and these are defined at **User and Device > Device > Device Definitions.** This parameter can limit the devices that can connect to this policy to those specific MAC addresses that are already known by the FortiGate and are approved for the policy.

Destination address

In the same way that the source address may need to be limited, the destination address can be used as a traffic filter. When the traffic is destined for internal resources the specific address of the resourece can be defined to better protect the other resources on the network. One of the specialized destination address options is to use a Virtual IP address. The destination address doesn't need to be interal you can define policies that are only for connecting to specific addresses on the Internet.

Schedule

The time frame that is applied to the policy. This can be something as simple as a time range that the sessions are allowed to start such as between 8:00 am and 5:00 pm. Something more complex like business hours that include a break for lunch and time of the session's initiation may need a schedule group because it will require multiple time ranges to make up the schedule.

Service

The service or service chosen here respresent the TCP/IP suite port numbers that will most commonly be used to transport the named protocols or group of protocols. This will be a little different than Application Control which looks more closely at the packets to determine the actual protocol used to create them.

Without all six (possibly 8) of these things matching, the traffic will be declined. Each traffic flow requires a policy and the direction is important as well. Just because packets can go from point A to point B on port X does not mean that the traffic can flow from point B to point A on port X. A policy must be configured for each direction.

When designing a policy there is often reference to the traffic flow, but most communication is a two way connection so trying to determine the direction of the flow can be somewhat confusing. If traffic is HTTP web traffic the user sends a request to the web site, but most of the traffic flow will be coming from the web site to the user. Is the traffic flow considered to be from the user to the web site, the web site to the user or in both directions? For the purposes of determining the direction for a policy the important factor is the direction of the initiating communication. The user is sending a request to the web site so this is the initial communication and the web site is just responding to it so the traffic will be from the users network to the Internet.

A case where either side can initiate the communication like between two internal interfaces on the FortiGate unit would be a more likely situation to require a policy for each direction.

What is not expressly allowed is denied

One of the fundamental ideas that can be found in just about any firewall is the rule than anything that is not expressly allowed is by default denied. This is the foundation for any strategy of protecting your network. Right

out of the box, once you have your FortiGate device connected into your network and hooked up with your ISP your network is protected. Nothing is getting out or in so it is not very convenient, but you don't have to worry that between the time you hooked it up and the point that you got all of the policies in place that someone could have gotten in and done something to your resources. The reason that this needs to be kept in mind when designing policies is because you cannot assume that any traffic will be allowed just because it makes sense to do so. If you want any kind of traffic to make it past the FortiGate firewall you need to create a policy that will allow that traffic. To maintain the protection of the network should also make sure that the any policy you create allows only the traffic you intend to go only to where you specifically want it to go and when you want it to go there.

Example

You have a web server on your network that is meant to provide a collaborative work environment web site for your employees and a partner company for a project over the course of the next 3 months.

It is theoretically possible to allow connections into your network to any device on that network for any service and at any time. The problem with this is that we might not want just anybody looking at those resources. Sadly, no matter how much it is wished otherwise, not everybody on the Internet can be trusted. Which means we now have to be very specific in our instructions as to what traffic to allow into the network. Each step that we take towards being more specific as to what we allow means that there is that much more that is not allowed and the level of protection of a resources is directly proportional to the amount of traffic that is not allowed. If somebody can't get at it they can't damage or steal it.

Limiting where the traffic is allowed to go to means that other computers on your network besides the web-server are protected.

- Limiting where the traffic is allowed to come from means that, if feasible, you can limit the systems that can access the web server to just employees or the partner company computers.
- Limiting the services to just web traffic means that a malicious person, even if they were connection from a computer at the partner organization could only use the features of web traffic to do anything malicious.
- Limiting the policy to the time span of the project would mean that even if the IT department forgot to remove the policy after the end of the project than no computer from the other company could be used to do anything malicious through the policy that allowed the traffic.

This is just a very basic example but it shows the underlying principles of how the idea that anything not expressly allowed is by default denied can be used to effectively protect your network.

Policy order

Another important factor in how firewall policies work is the concept of precedence of order or if you prefer a more recognizable term, "first come, first served".

It is highly likely that even after only a relatively small number of policies have been created that there will be some that overlap or are subsets of the parameters that the policies use to determine which policy should be matched against the incoming traffic. When this happens there has to be a method to determine which policy should be applied to the packet. The method which is used by most firewalls it based on the order of the sequence of the policies.

If all of the policies were placed in a sequential list the process to match up the packet would start at the top of the list and work its way down. It would compare information about the packet, specifically these points of information:

1. The interface the packet connected to the FortiGate firewall
2. The source address of the packet, and possibly the sending user and device.
3. The destination address of the packet

4. The interface the packet would need to use to get to the destination address based on the routing table
5. The port the packet is destined for
6. The time that the packet connected to the FortiGate

As soon as the a policy is reached that matches all of the applicable parameters, the instructions of that policy are applied and the search for any other matching policies is stopped. All subsequent policies are disregarded. Only 1 policy is applied to the packet.

If there is no matching policy among the policies that have been configured for traffic the packet finally drops down to what is always the last policy. It is an implicit policy. One of a few that are referred to by the term “policy0”. This policy denies everything.

The implicit policy is made up of the following settings:

- Incoming Interface: any
- Source Address: any
- Outgoing Interface: any
- Destination Address: any
- Action: DENY

The only setting that is editable in the implicit policy is the logging of violation traffic.

A logical best practice that comes from the knowledge of how this process works is to make sure that the more specific or specialized a policy is, the closer to the beginning of the sequence it should be. The more general a policy is the higher the likelihood that it could include in its range of parameters a more specifically targeted policy. The more specific a policy is, the higher the probability that there is a requirement for treating that traffic in a specific way.

Example

For security reasons there is no FTP traffic allowed out of a specific subnet so there is a policy that states that any traffic coming from that subnet is denied if the service is FTP, so the following policy was created:

Policy #1

Source Interface	Internal1
Source Address	192.168.1.0/24
Source User(s)	<left at default setting>
Source Device Type	<left at default setting>
Outgoing Interface	WAN1
Destination Address	0.0.0.0/0.0.0.0
Service	FTP
Schedule	always
Action	deny

Now as these things usually go it turns out that there has to be an exception to the rule. There is one very secure computer on the subnet that is allowed to use FTP and once the content has been checked it can them be distributed to the other computer on the subnet. So a second firewall policy is created.

Policy #2

Source Interface	Internal1
Source Address	192.168.1.38/32
Source User(s)	<left at default setting>
Source Device Type	<left at default setting>
Outgoing Interface	WAN1
Destination Address	0.0.0.0/0.0.0.0
Service	FTP
Schedule	always
Action	Allow

By default, a policy that has just been created will be placed last in the sequence so that it is less likely to interfere with existing policies before it can be moved to its intended position. If you look at Policy #2 you will notice that it is essentially the same as Policy #1 exempt for the Source Address and the Action. You will also notice that the Source Address of the Policy #2 is a subset of the Source address in policy #1. This means that if nothing further is done, Policy #2 will never see any traffic because the traffic will always be matched by Policy #1 and processed before it has a chance to reach the second policy in the sequence. For both policies to work as intended Policy #2 needs to be moved to before Policy #1 in the sequence.

Exception to policy order

There is a relevant exception to the normal policy order. Policies with VIPs don't appear to behave the same way. Traffic that is handled by VIPs is processed through the associated policy before the traffic is checked against other policies in the usual top down order.

This only appears inconsistent with the policy order rule because when handling the traffic, firewall policies are not the first thing checked. VIP translations are checked first, and if there is more than one VIP that the traffic fits, it is handled in the top down order that is followed by policies. If the traffic is not claimed by a policy in the VIP translation phase, it is checked against the routing rules. If it passes the routing checks, the traffic is allowed to be controlled by the polices.

This processing of traffic targeting a VIPs only applies if there is a policy that included the VIP and the traffic matches all of the criteria checks. There is no need to worry about creating VIPs that are not controlled by a policy.

There are security implications associated with this behavior. Administrators could assume that a policy will process traffic before it drops down to a policy with a VIP in it. This can allow traffic to pass through the firewall into a part of the network that it was not intended for, if it was to be allowed in at all. The way to prevent traffic being incorrectly allowed through a policy containing a VIP is to have that policy be more restrictive or to have a separate policy containing the same VIP deny the traffic earlier in the sequence.

As proof of the behaviour, look at the following traffic analysis of a packet sent to a VIP. You will see that the packet is translated even before it is allowed to pass through the firewall by a policy.

```
2015-06-10 06:33:21 id=20085 trace_id=1 func=print_pkt_detail line=4373 msg="vd-root
    received a packet(proto=6, 24.114.222.34:51434->24.212.230.77:3389) from wan1. flag
    [S], seq 1579917634, ack 0, win 8192"
2015-06-10 06:33:21 id=20085 trace_id=1 func=init_ip_session_common line=4522
    msg="allocate a new session-01480894"
2015-06-10 06:33:21 id=20085 trace_id=1 func=fw_pre_route_handler line=174 msg="VIP-
    10.10.66.2:3389, outdev-wan1"
2015-06-10 06:33:21 id=20085 trace_id=1 func=__ip_session_run_tuple line=2534 msg="DNAT
    24.212.230.77:3389->10.10.66.2:3389"
2015-06-10 06:33:21 id=20085 trace_id=1 func=vf_ip4_route_input line=1596 msg="find a
    route: flags=00000000 gw-10.10.66.2 via internal5"
2015-06-10 06:33:21 id=20085 trace_id=1 func=fw_forward_handler line=670 msg="Allowed by
    Policy-15:"
```

Policy identification

When looking at the policy listing it can appear as if the policies are identified by the sequence number in the far left column. The problem is that this number changes as the position of the policy in the sequence changes. The column that correctly identifies the policy, and the value sticks with the policy is the "ID" column. This column is not shown by default in the listing but can be added to the displayed columns by right clicking on the column heading bar and selecting it from the list of possible columns.

When looking in the configuration file the sequence is based upon the order of the policies as they are in the file just as they are in the list in the GUI. However, if you need to edit the policy in the CLI you must use the ID number.

UUID support

Universally Unique Identifier (UUID) attributes have been added to policies to improve functionality when working with FortiManager or FortiAnalyser units. If required, the UUID can be set manually through the CLI.

CLI syntax:

```
config firewall {policy/policy6/policy46/policy64}
   edit 1
      set uuid <example uuid: 8289ef80-f879-51e2-20dd-fa62c5c51f44>
      next
   end
```

Security profiles

Where security policies provide the instructions to the FortiGate unit for controlling what traffic is allowed through the device, the Security profiles provide the screening that filters the content coming and going on the network. Security profiles enable you to instruct the FortiGate unit about what to look for in the traffic that you don't want, or want to monitor, as it passes through the device.

A security profile is a group of options and filters that you can apply to one or more firewall policies. Security profiles can be used by more than one security policy. You can configure sets of security profiles for the traffic types handled by a set of security policies that require identical protection levels and types, rather than repeatedly configuring those same security profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict antivirus protection, traffic between trusted internal addresses might need moderate antivirus protection. To provide the different levels of protection, you might configure two separate profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

Security profiles are available for various unwanted traffic and network threats. Each are configured separately and can be used in different groupings as needed. You configure security profiles in the Security Profiles menu and applied when creating a security policy by selecting the security profile type.

There is a separate handbook for the topic of the Security Profiles, but because the Security Profiles are applied through the Firewall policies it makes sense to have at least a basic idea of what the security profile do and how they integrate into the FortiGate's firewall policies. The following is a listing and a brief description of what the security profiles offer by way of functionality and how they can be configured into the firewall policies.

AntiVirus

Antivirus is used as a catch all term to describe the technology for protection against the transmission of malicious computer code sometimes referred to as malware. As anyone who has listened to the media has heard that the Internet can be a dangerous place filled with malware of various flavours. Currently, the malware that is most common in the Internet, in descending order, is Trojan horses, viruses, worms, adware, back door exploits, spyware and other variations. In recent years, not only has the volume of malicious software become greater than would have been believed when it first appeared but the level of sophistication has risen as well.

The Antivirus Filter works by inspecting the traffic that is about to be transmitted through the FortiGate. To increase the efficiency of effort it only inspects the traffic being transmitted via the protocols that it has been

configured to check. Before the data moves across the FortiGate firewall from one interface to another it is checked for attributes or signatures that have been known to be associated with malware. If malware is detected, it is removed.

Web filtering

Malicious code is not the only thing to be wary of on the Internet. There is also the actual content. While the content will not damage or steal information from your computer there is still a number of reasons that would require protection from it.

In a setting where there are children or other sensitive people using the access provided by a connected computer there is a need to make sure that images or information that is not appropriate is not inadvertently displayed to them. Even if there is supervision, in the time it takes to recognize something that is inappropriate and then properly react can expose those we wish to protect. It is more efficient to make sure that the content cannot reach the screen in the first place.

In an organizational setting, there is still the expectation that organization will do what it can to prevent inappropriate content from getting onto the computer screens and thus provoking an Human Resources incident. There is also the potential loss of productivity that can take place if people have unfiltered access to the Internet. Some organizations prefer to limit the amount of distractions available to tempt their workers away from their duties.

The Web filter works primarily by looking at the destination location request for a HTTP(S) request made by the sending computer. If the URL is on a list that you have configured to list unwanted sites, the connection will be disallowed. If the site is part of a category of sites that you have configured to deny connections to the session will also be denied. You can also configure the content filter to check for specific key strings of data on the actual web site and if any of those strings of data appear the connection will not be allowed.

Application control

Application control is designed to allow you to determine what applications are operating on your network and to the also filter the use of these applications as required. Application control is also for outgoing traffic to prevent the use of applications that are against an organization’s policy from crossing the network gateway to other networks. An example of this would be the use of proxy servers to circumvent the restrictions put in place using the Web Filtering.

Intrusion protection (IPS)

Intrusion Prevention System is almost self explanatory. In the same way that there is malware out on the Internet that the network needs to be protected from there are also people out there that take a more targeted approach to malicious cyber activity. No operating system is perfect and new vulnerabilities are being discovered all of the time. An intrusion prevention system is designed to look for activity or behavior that is consistent with attacks against your network. When attack like behavior is detected it can either be dropped or just monitored depending on the approach that you would like to take.

As new vulnerabilities are discovered they can be added to the IPS database so that the protection is current.

Email filtering

Spam or unsolicited bulk email is said to account for approximately 90% of the email traffic on the Internet. Sorting through it is both time consuming and frustrating. By putting an email filter on policies that handle email traffic, the amount of spam that users have to deal with can be greatly reduced.

Data Leak Prevention (DLP)

Data Leak Prevention is used to prevent sensitive information from leaving your network. When people think of security in the cyber-world one of the most common images is that of a hacker penetrating your network and making off with your sensitive information, but the other way that you can lose sensitive data is if someone already on the inside of your network sends it out. This does not have to be an act of industrial espionage. It can just be a case of not knowing the policies of the organization or a lack of knowledge of security or laws concerning privacy.

For instance, a company may have a policy that they will not reveal anyone's Social Security number, but an employee emails a number of documents to another company that included a lengthy document that has a Social Security number buried deep within it. There is not malicious intent but if the information got out there could be repercussions.

If an organization has any information in a digital format that it cannot afford for financial or legal reasons, to leave its network, it makes sense to have Data Leak Prevention in place as an additional layer of protection.

VoIP

Voice over IP is essentially the protocols for transmitting voice or other multimedia communications over Internet Protocol networks such as the Internet. The Security Profiles VoIP options apply the SIP Application Level Gateway (ALG) to support SIP through the FortiGate unit. The SIP ALG can also be used to protect networks from SIP-based attacks.

ICAP

Internet Content Adaptation Protocol (ICAP) off loads HTTP traffic to another location for specialized processing. The purpose of this module when triggered is to send the incoming HTTP traffic over to a remote server to be processed thus taking some of the strain off of the resources of the FortiGate unit. The reasons for the specialized process could be anything from more sophisticated Antivirus to manipulation of the HTTP headers and URLs.

EndPoint control

EndPoint Control makes sure that certain standards are kept. When a computer on the Internet becomes connected to the FortiGate unit by VPN that computer is now part of the same network and therefore needs to be subject to the same levels of protection, not only to protect the computer but the network. In the EndPoint Control section you can set the minimum standards for things like AntiVirus software and VPN software.

Proxy option components

Any time a security profile that requires the use of a proxy is enabled the Proxy Options field will be displayed. Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out and so the Proxy Options are there to define the parameters of how the traffic will be processed and to what level the traffic will be processed. In the same way that there can be multiple security profiles of a single type there can also be a number of unique Proxy Option profiles so that as the requirements for a policy differ from one policy to the next you can also configure a different Proxy Option profile for each individual policy or you can use one profile repeatedly.

The Proxy Options refer to the handling of the following protocols:

- HTTP
- SMTP

- POP3
- IMAP
- FTP
- NNTP
- MAPI
- DNS
- IM

The configuration for each of these protocols is handled separately.

It should also be noted that these configurations apply to only the Security Profiles Proxy-based processes and not the Flow-based processes.

The use of different proxy profiles and profile options

Just like other components of the FortiGate, there is the option for different Proxy Option profiles so that you can be very granular in your control of the workings of the FortiGate. In the case of the Proxy Option profiles the thing that you will want to focus on is the matching up of the correct profile to a firewall policy that is using the appropriate protocols. If you are creating a Proxy Option profile that is designed for policies that control SMTP traffic into your network you only want to configure the settings that apply to SMTP. You do not need or want to configure the HTTP components.

Oversized file log

This setting is for those that would like to log the occurrence of oversized files being processed. It does not change how they are processed it only enables the FortiGate unit to log that they were either blocked or allowed through. A common practice is to allow larger files through without antivirus processing. This allows you to get an idea of how often this happens and decide on whether or not to alter the settings relating to the treatment of oversized files.

The setting of the threshold for what is considered to be an oversized file is located in the Oversized File / Email Threshold that is found in some of the protocol options for the Proxy Options.

Protocol port mapping

While each of the protocols listed has a default TCP port that is commonly used, the level of granularity of control on the FortiGate firewall allows that the port used by the protocols can be individually modified in each separate Profile. It can also be set to inspect any port with flowing traffic for that particular protocol. The headers of the packets will indicate which protocol generated the packet. To optimize the resources of the unit the mapping and inspection of protocols can be enabled or disabled depending on your requirments.

Comfort Clients

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit begins scanning the file. During the buffering and scanning procedure, the user must wait. After the scan is completed, if no infection is found, the file is sent to the next step in the process flow. If the file is a large one this part of the process can take some time. In some cases enough time that some users may get impatient and cancel the download.

The comfort client feature to mitigates this potential issue by feeding a trickle of data while waiting for the scan to complete so as to let the user know that processing is taking place and that there hasn't been a failure in the

transmission. This slow transfer rate continues until the antivirus scan is complete. Once the file has been successfully scanned without any indication of viruses the transfer will proceed at full speed.

If there is evidence of an infection the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file. If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS and FTPS traffic.

Buffering the entire file allows the FortiGate unit to eliminate the danger of missing an infection due to fragmentation because the file is reassembled before examination. Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

Oversized file/email threshold

This is another feature that is related to antivirus scanning. The FortiGate unit has a finite amount of resources that can be used to buffer and scan a file. If a large file such as an ISO image or video file was to be downloaded this could not only overwhelm the memory of the FortiGate, especially if there were other large files being downloaded at the same time, but could exceed it as well. For this reason, how to treat large files needs to be addressed.

A threshold is assigned to determine what should be considered an oversize file or email. This can be set at any size from 1 MB to 50 MB. Any file or email over this threshold will not be processed by the Antivirus Security Profiles. Once a file is determined to be oversized it must be then determined whether to allow it or to block it.

These settings are not a technical decision but a policy one that will depend on your comfort level with letting files into your network. As there often is, there is a compromise between convenience or ease of use and security. If you want to go for a high peace of mind level you can configure the firewall to block oversized files and thus no files would be coming into the network that have not been scanned. If you are looking for optimizing the memory of the FortiGate unit and making sure that everybody is getting the files they want, you can lower the threshold and allow files that are over the threshold.

It should be noted that in terms of probability that malware is more likely to be found in smaller files than in larger files. A number of administrators take this into account when they lower the default threshold so as to lessen the impact on memory if they see the FortiGate unit going into conserve mode on a regular basis.

Chunked bypass

The HTTP section allows the enabling of “Chunked Bypass”. This refers to the mechanism in version 1.1 of HTTP that allows a web server to start sending chunks of dynamically generated output in response to a request before actually knowing the actual size of the content. Where dynamically generated content is concerned this means that there is a faster initial response to HTTP requests. From a security stand point it means that the content will not be held in the proxy as an entire file before proceeding.

Allow fragmented messages

The specifications of RFC 2046 allow for the breaking up of emails and sending the fragments in parallel to be rebuilt and read at the other end by the mail server. It was originally designed to increase the performance over slower connections where larger email messages were involved. It will depend on your mail configuration if this is even possible for your network but outside of Microsoft Outlook and Outlook Express, not many email clients are set up to break up messages like this. The drawback of allowing this feature is that if malware is broken up between multiple fragments of the message the risk is run that it will not be detected by some antivirus configurations because the code may not all be present at the same time to identify.

Append email signature

The Append Email Signature is used when an organization would like to ensure that over and above our in this case underneath the existing personal signatures of the sender, all of the emails going out of their network have the appropriate “boilerplate”, for lack of a better term. These appended emails do not replace existing signatures. They are as the feature states, appended to the email.

Examples could include things like:

- Without prior approval the email should not be forwarded.
- Please be environmentally friendly and don’t print out emails
- For questions regarding the purchasing of our products please call…

It can be anything that the organization would like as long as it is in text format. The use of this feature usually works best in an environment where there is some standardization of what goes into the personal signatures of the senders so that there is no duplication or contradiction of information in the signatures.

SSL/SSH inspection

While the profile configuration for this is not found in the Security Profiles section but in the Policy Section, it is set in the policy along with the security profiles. This sort of analysis is some times referred to as deep scanning.

Deep Inspection works along the following lines. If your FortiGate unit has the correct chipset it will be able to scan SSL encrypted traffic in the same way that regular traffic can be scanned. The FortiGate firewall will essentially receive the traffic on behalf of the client and open up the encrypted traffic. Once it is finished it re-encrypts the traffic and sends it on to its intended recipient. It is very similar to a man-in-the-middle attack. By enabling this feature, it allows the FortiGate firewall to filter on traffic that is using the SSL encrypted protocol.

The encrypted protocols that can be inspected are:

- HTTPS
- SMTPS
- POP3S
- IMAPS
- FTPS

Before the invention of SSL inspection, scanning regular web traffic can be circumvented by using the prefix https:// instead of http:// in the URL. SSL inspection prevents this circumvention. However, because when the encrypted traffic is decrypted it has to be re-encrypted with the FortiGate’s certificate rather than the original certificate it can cause errors because the name on the certificate does not match the name on the web site.

At one point deep inspection was something that was either turned on or off. Now individual deep inspection profiles can be created depending on the requirements of the policy. Depending on the Inspection Profile, you can:

- Configure which CA certificate will be used to decrypt the SSL encrypted traffic.
- Configure which SSL protocols will be inspected.
- Configure which ports will be associated with which SSL protocols for the purpose of inspection.
- Configure which websites will be exempt from SSL inspection
- Configure whether or not to allow invalid SSL certificates.
- Configure whether or not SSH traffic will be inspected.

HTTP Strict Transport Security (HSTS) Protocol

HSTS is a protocol used by Google and other web browsers to prevent man-in-the-middle attacks.

When performing deep inspection, the FortiGate intercepts the https traffic and would send its own self-signed CA certificate to the browser. If the browser is configured to use HSTS connections, it would refuse the FortiGate CA certificate since it is not on the trusted list for Google servers.

To keep the CA certificate from being refused, the HSTS settings should be cleared from the browser. Instructions for this vary between browsers.

Inspection exemption

When you are using a browser to visit SSL encrypted sites and we are using a certificate that does not match the certificate of the site, we are presented with a warning message and the option of continuing, using the untrusted certificate, or terminating the session. However, there are a number of applications that use SSL encrypted traffic. If the application detects SSL traffic that wasn't signed with a certificate that it trusts it will not allow the traffic. The applications do not give the option to manually indicate that we trust the certificate or the site.

If the option is available, the customer may choose to import needed SSL certificates into Local Certificates and configure a policy for communication for that application.

The assist in preventing loss of access to these site but still enabling the SSL inspection of the rest of the internet traffic, a method of exempting either Website categories or specific sites has been developed. To exempt a large group of sites the profile can be configure to exempt FortiGuard Categories. There are 3 of these categories preselected due to the high likelihood of issues with associated applications with the type of websites included in these categories.

- Heath and Wellness
- Personal Privacy
- Finance and Banking

Other more specific websites can be added to the exemption list by creating addresses for them at **Policy & Objects > Objects > Addresses**. The adding of addresses is done by selection from a drop down menu. There is an option at the bottom of the list to create a new address, but otherwise only preconfigured addresses that are configured to be on the "Any" interface will be available for selection.

Examples of sites that you may want to configure for exemption so that there will be no interference due to certificate issues:

Apple

- *.appstore.com
- *.apple.com
- *.itunes.apple.com
- *.icloud.com
- swscan.apple.com

Dropbox

- *.dropbox.com

Skype

- *.messenger.live.com

Windows Updates

- update.microsoft.com

Allow invalid SSL certificate

This setting was something that used to be part of the **Proxy Options**, but now that SSL inspection has it's own configuration setting it is configured with those. It might seem like a straight forward decision that the allowing of invalid SSL certificates must be bad and therefore should not be allowed, but there can be some reasons that should be considered. The issues at hand are the reasons to use a SSL certificate and the reasons that a certificate will be considered invalid.

At a purely technical level, a properly formed certificate will encrypt the data so that it can only be read by the intended parties and not be read by anyone sniffing traffic on the network. For this reason, people will often use self-signed certificates. These self signed certificates are free and will encrypt the data just as well as those purchased from any of the big vendors of certificates, but if they are not listed as an approved Certificate Authority (CA) the certificates will be considered invalid.

On the other hand, one of the services the vendors provide is verification of identity of those that purchase their certificates. This means that if you see a valid certificate from a site that identified itself as being from "valid-company.com" that you can be reasonably sure that the site does belong to that company and not a false site masquerading as being part of that company.

Creating or editing an SSL/SSH inspection profile

1. Go to **Policy & Objects > Policy > SSL/SSH Inspection**.
   This will open to one of the existing profiles.
   The links for the actions are located in the upper right hand corner of the window.
   - To view a list of the exiting profiles select the List icon (a page) at the far right.
   - To clone an existing profile, select the Clone icon (one page behind another), second from the right
   - To create a new profile, select the Create New icon ("+ "symbol), third from the right.
   - To view or edit an existing profile, choose it from the dropdown menu field.
2. **Name Field:**
   Give the Profile an easily identifiable name that references its intent.

3. **Comments Field:**
   Enter any additional information that might be needed by administrators, as a reminder of the profile's purpose and scope.
4. **SSL Inspection Options:**
   a. Enable SSL Inspection of:
   - Multiple Clients Connecting to Multiple Servers - Use this option for generic policies where the destination is unknown.
   - Protecting SSL Server - Use this option when setting up a profile customized for a specific SSL server with a specific certificate.

   b. CA Certificate
   Use the drop down menu to choose which one of the installed certificates to use for the inspection of the packets.

   c. Inspection Method
   The options here are:
   - SSL Certificate Inspection - only inspects the certificate, not the contents of the traffic.
   - Full SSL Inspection - inspects all of the traffic.

   d. Inspect All Ports
   Enable the ability to inspect all ports by checking the box. If the feature is not enabled, specify in the field next to the listed protocols, the port through which that protocols traffic will be inspected. Traffic of that protocol going through any other port will not be inspected.
5. **Exempt from SSL Inspection:**
   Use the dropdown menus in this section to specify either a FortiGuard Web Category or addresses that will be exempt from SSL inspection.
   a. Web Categories
   By default the categories of Health and Wellness, Personal Privacy, and Finance and Banking have been added as these are one that are most likely to have applications that will require a specific certificate.

   b. Addresses
   These can be any of the Address objects that have an interface of "Any".
6. **SSH Inspection Options:**
   a. SSH Deep Scan
   Toggle the grey on button so that it is:
   Greyed out to disable the feature
   Opaque and vibrate to enable the feature

   b. SSH Port
   The available options are:
   - **Any** - choosing this option will search all of the traffic regardless of service or TCP/IP port for packets that conform to the SSH protocol
   - **Specify** - choosing this option will restrict the search for SSH protocol packets to the TCP/IP port number specified in the field. This is not as comprehensive but it is easier on the performance of the firewall.

   d. Protocol Actions
   - Exec - Block, Log or neither. Select using check boxes.
   - Port-Forward - Block, Log or neither. Select using check boxes.
   - SSH-Shell - Block, Log or neither. Select using check boxes.
   - X11-Filter - Block, Log or neither. Select using check boxes.

7. **Common Options:**
   a. Allow Invalid SSL Certificates
   Check the box to enable the passing of traffic with invalid certificate
   b. Log Invalid Certificates
   Check the box to have the Logging function record traffic sessions that contained invalid certificates

The **Enable SSH Deep Scan** feature is enabled by default when creating a new SSL/SSH Inspection profile. There are situations were this feature can cause issues so be sure that you would like it enabled before applying it.

The context location for configuring the SSL/SSH Inspection in the CLI is:

```
config firewall ssl-ssh-profile
```

Viewing firewall policies

When you first go into the Policy window, found by going to Policy > Policy > Policy, you will see a table with a menu bar across the top. The menu bar will have the following items:

At the top left:

- Create New (with a “+” sign on the left and a downward pointing triangle on the right)
- Clone
- Delete
- Column Settings
- Filter Settings

At the top right:

- Section View
- Global View

The items at the top right with their radio buttons represent the 2 potential views that the policies can be displayed in.

The Global View shows all of the policies in the order of their sequence. With the default settings you will be able to see the sequence number in a column close to the left side of the table.

The Section view is similar to the Global View except that as the name implies it is divided into sections. By default the sections are based on the paths between the interfaces. These can be referred to as “interface pairings”. For instance, all of the policies referencing traffic from WAN1 to DMZ will be in one section. The policies referencing traffic from DMZ to WAN1 will be in another section.

The sections are collapsible so that you only need to look at the sections with policies you are interested in. It is possible to add customized subsections within the default sections of interface pairings. This would be useful in a situation where you have a lot of policies and would like to further compartmentalize them by common attributes so that things are easier to find.

The default column headings are:

- [Check box icon]
- Seq.#
- Source
- Destination
- Authentication
- Schedule
- Service
- Action
- Log

The column that are shown are configurable. All but the first 2 can be removed or their position changed. There are also a number of other columns that display information about the policies that can be added. One of the more useful ones that can be added is the ID column. The reason for adding this one is that policies are referenced by their ID number for simplicity and ease of administration. If you are looking in the CLI you will see that the only designation for a policy is its number and if you wish to change the order of a policy you will be asked to move it before or after another policy by referencing its number.

How “Any” policy can remove the section view

The FortiGate unit will automatically change the view on the policy list page to Global View whenever a policy containing “any” in the Source interface/zone or Destination interface/zone is created. If the Section View is greyed out it is likely that one or more of the policies has “any” as a Source or Destination interface.

With the use of the “any” the policy should go into multiple sections because it could effectively be any of a number of interface pairings. As mentioned, policies are sectioned by using the interface pairings (for example, port1 -> port2) and each section has its own specific policy order. The order in which a policy is checked for matching criteria to a packet’s information is based solely on the position of the policy within its section or within the entire list of policies as a whole but if the policy is in multiple sections at the same time there is no mechanism for placing the policy in a proper order within all of those sections at the same time because it is a manual process and there is no parameter to compare the precedence of one section or policy over the other. Thus a conflict is created. In order to resolve the conflict the FortiGate firewall removes that aspect of the sections so that there is no need to compare and find precedence between the sections and it therefore has only the Global View to work with.

Security policy configuration extensions

When first creating the policy the configuration form will ask for a choice between the policy types of Firewall or VPN, Firewall being the default. Choosing whether or not to leave the selection as Firewall is straight forward. If the policy is not a policy based VPN policy then it is a Firewall policy type.

There are essentially 2 types of VPN connections, Interface Based and Policy Based. In an Interface Based VPN tunnel a logical interface is created that can be seen as an interface by the policies in the same way that any of the physical interfaces can be seen. Therefore to govern the traffic a regular policy will work. The policy based VPN tunnels work slightly different and therefore need a slightly different policy configuration. For a more detail explanation of the difference between the types of VPN tunnels refer to the VPN documentation found in the VPN handbooks or in the VPN section of the Complete Administration Guide.

Once either the Firewall or the VPN type has been chosen there is then a choice between one of subtypes for each of the Policy types. For the Firewall type of policy the subtypes are:

- Address
- User Identity

- Device Identity

The Address subtype refers to policies where access through the FortiGate firewall is dependant on the source location of the addresses of the devices involved in the traffic matched to the policy.

The User Identity subtype refers to policies where access through the FortiGate firewall is dependant on the users credentials or Identity.

The Device Identity subtype refers to policy where access through the FortiGate firewall is dependant on the specific device being used based on the MAC address of the device or belonging to a group of devices that are based on device types or belonging to custom made groups.

For the VPN type the subtypes are:

- IPsec
- SSL-VPN

As expected the two subtypes are the two different types of VPN tunnels that the FortiGate firewall supports in a policy based configuration.

Identity-based policies

Identity based policies are ones in which there is the additional component of either an account identity or device identity. The inclusion of one or both of these components adds an extra dimension of complexity to working with these policies in the context of the other policies so while the extra security and granularity of control are beneficial, extra care must be taken when configuring the policies themselves and how they are positioned in the policy sequence. The actual configuration of these identities are explained in detail in the Authentication Handbook.

Identity-based security policies are usually configured for IPsec or SSL VPN traffic since this type of traffic usually requires authentication from network users.

Identity-based policy positioning

In non-identity based policies, if non of the 6 mandatory policy parameters matches the header of the traffic packets the parameters are compared against the next policy in sequence. Because those parameters are mandatory there is always a value to test against and whether or not the policy applies is certain. The fact that the identity parameters are not required makes knowing whether or not the correct policy will be applied less obvious.

Originally, the identity aspect of a policy was an entire sub-policy checking sequence within each policy, including its own 0 policy at the end of the sequence. If all of the other parameters match the policy would then compare the traffic's identity with the list of identity groups in the policy starting at the beginning of the sequence and going through them until an identity was found that matched and then the rules for that identity group would be applied. If the traffic's identity did not match any of those listed in the policy it go to the last identity in the policy would be everyone and the Action would be deny.

The identity aspects of policies have now been incorporated in a single flat configuration that makes them a fundamental part of the policy rather than something that is added to the policy. This is simpler and allows for more complex combinations of address identification, user authentication and device determination that were not possible with previous policy configurations. Both user groups and device groups can be part of the same policy. Because the identity aspects are optional, more flexibility in creating policies that use authentication is possible.

Identity fall through rules

The fall through rules for policies in 5.2 have changed so that they are more in keeping with the practices of other vendors. This makes it easier for users used to other firewalls to configure the policies and it also makes it simpler to convert the policies of other firewalls to be used on a FortiGate firewall.

Previously, if traffic reached an identity policy and the user or device was not a member of one of the groups specified it would fall through to the implicit deny all policy. This meant that any traffic that reached that policy would have to be authenticated and a member of one of the listed groups. If the 6 required parameters matched, the traffic would not be getting past this policy.

The approach is now to treat the the identity parameters, if they exist, the same as the other parameters, in that if they do not match any listed in the policy, the traffic drops down to the next policy.

Example:

There are three policies where all the parameters are the same except:

- Policy # 1 - Source User Group A is assigned profile A
- Policy # 2 - Source User Group B s assigned profile B
- Policy # 3 - Source User(s) and Source Device Type are empty

Traffic that matches all of the required parameters will be processed as follows:

- Traffic authenticated as being from User Group A will be processed by Policy # 1.
- Traffic authenticated as being from User Group B will be processed by Policy # 2.
- Traffic with no authenticated users will be processed by Policy # 3.
- Traffic authenticated as being from User Group C will be processed by Policy # 3.

In the methodology before FortiOS 5.2, traffic authenticated as being User Group B, User Group C or no authenticated user at all would have been stopped at Policy # 1.

The CLI command “fall-through-unauthenticated” that was added in 5.0.1 attempted to allow a process similar to this, but only applied to unathenticated traffic and not authenticated traffic that didn’t match the list of groups is the sub-policy. The current methodology is not subject to the same limitation and alleviates the need for the function of this command so the command has been removed from the CLI.

Implicit protocols

In previous versions of the firmware, the protocols that were used to authenticate such as HTTP, HTTPS, FTP, and Telnet, were supported on the policy whether or not they were included in the supported services. In 5.2, the protocol needed to authenticate needs to be included in the list of allowed services in order the the authentication to take place.

For example, if you have a VIP coming into your network that is for connecting to some security webcams located in your data center that use custom services or ports to connect to, if you are using an identity policy you would also have to include HTTP or HTTPS in the services list in order to actually authenticate.

Another formerly implicit protocol that is not supported automatically in 5.2 is port 53 (DNS). If you are limiting the services of a protocol to web based protocols such as HTTP or HTTPS don’t forget to to add DNS so that the domain names can be resolved.

When upgrading the firmware from version 5.0.x to 5.2.x, a policy with either an identity or device sub-policy will automatically convert from a single policy with sub-policies to a separate policy for each identity based sub-policy.

VPN policies

At one point, if you wanted to have secure digital communications between 2 points a private network would be created. This network would only allow the people that were intended to get the communications on it. This is very straightforward if the 2 points are in the same room or even in the same building. It can all be done physically. If you are supposed to be on the secure network

VPNs are an answer to one of today's biggest concerns, how to make digital communications secure between to points that must communicate over the Internet which anybody can have access to

IPsec policies

IPsec policies allow IPsec VPN traffic access to the internal network from a remote location. These policies include authentication information that authenticates users and user group or groups. These policies specify the following:

- the FortiGate firewall interface that provides the physical connection to the remote VPN gateway, usually an interface connected to the Internet
- the FortiGate firewall interface that connects to the private network
- IP addresses associated with data that has to be encrypted and decrypted
- optional: a schedule that restricts when the VPN can operate, and services (or types of data) that can be sent.

For a route-based (interface mode) VPN, you do not configure an IPsec security policy. Instead, you configure two regular ACCEPT security policies, one for each direction of communication, with the IPsec virtual interface as the source or destination interface, as appropriate.

Interface policies

Interface policies are implemented before the "security" policies and are only flow based.

This feature allows you to attach a set of IPS policies with the interface instead of the forwarding path, so packets can be delivered to IPS before entering firewall. This feature is used for following IPS deployments:

- One-Arm: by defining interface policies with IPS and DoS anomaly checks and enabling sniff-mode on the interface, the interface can be used for one-arm IDS;
- IPv6 IPS: IPS inspection can be enabled through interface IPv6 policy. Only IPS signature scan is supported in FortiOS 5.2. IPv6 DoS protection is not supported;
- Scan traffics that destined to FortiGate;
- Scan and log traffics that are silently dropped or flooded by Firewall or Multicast traffic.

IPS sensors can be assigned to an interface policy. Both incoming and outgoing packets are inspected by IPS sensor (signature).

Here is an example of an interface policy,

```
config firewall interface-policy
   edit 1
      set status enable
```

```
        set interface "port14"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set application-list-status disable
        set ips-sensor-status enable
        set ips-sensor "default"
        set av-profile-status disable
        set webfilter-profile-status disable
        set spamfilter-profile-status disable
        set dlp-sensor-status disable
        set label "Port 14 Interface Policy"
    next
end
```

DoS protection

Denial of Service (DoS) policies are primarily used to apply DoS anomaly checks to network traffic based on the FortiGate interface it is entering as well as the source and destination addresses. DoS checks are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system, so that legitimate users can no longer use it.

DoS policies are similar to firewall policies except that instead of defining the way traffic is allowed to flow, they keep track of certain traffic patterns and attributes and will stop traffic displaying those attributes. Further, DoS policies affect only incoming traffic on a single interface. You can further limit a DoS policy by source address, destination address, and service.

DoS configurations have been changed a couple of times in the past. In FortiOS 4.0, DoS protection was moved to the interface policy, so when it is enabled, it is the first thing checked when a packet enters FortiGate. Because of this early detection, DoS policies are a very efficient defence that uses few resources. Denial of service attacks, for example, are detected and its packets dropped before requiring security policy look-ups, antivirus scans, and other protective but resource-intensive operations.

A DoS policy examines network traffic arriving at an interface for anomalous patterns usually indicating an attack. This does not mean that all anomalies experience by the firewall are the result of an intentional attack.

Because an improperly configured DoS anomaly check can interfere with network traffic, no DoS checks are preconfigured on a factory default FortiGate unit. You must create your own before they will take effect. Thresholds for newly created sensors are preset with recommended values that you can adjust to meet the needs of your network.

To create a Denial of Service policy determine if it needs to be an IPv4 or IPv6 policy, then goto:

Policy & Objects > Policy > DoS Policy for IPv4.

Policy & Objects > Policy > IPv6 DoS Policy for IPv6.

It is important to know normal and expected network traffic before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could allow otherwise avoidable attacks.

Settings used in configuring DoS

Incoming interface

The interface to which this security policy applies. It will be the that the traffic is coming into the firewall on.

Source address

This will be the address that the traffic is coming from and must be a address listed in the Address section of the Firewall Objects. This can include the predefined “all” address which covers any address coming in on any interface. Multiple addresses or address groups can be chosen

Destination address

This will be the address that the traffic is addressed to. In this case it must be an address that is associated with the firewall itself. For instance it could be one of the interface address of the firewall, a secondary IP address or the interface address assigned to a Virtual IP address. Just like with the Source Address this address must be already configured before being used in the DoS policy.Multiple addresses, virtual IPs or virtual IP groups can be chosen.

Service

While the Service field allows for the use of the ALL service some administrators prefer to optimize the resources of the firewall and only check on the services that will be answered on an interface. Multiple services or service groups can be chosen.

Anomalies

The anomalies can not be configured by the user. They are predefined sensors set up for specific patterns of anomalous traffic

The anomalies that have been predefined for use in the DoS Policies are:

Anomaly Name	Description	Recommended Threshold
tcp_syn_flood	If the SYN packet rate of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
tcp_port_scan	If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second.
tcp_src_session	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
tcp_dst_session	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
udp_flood	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
udp_scan	If the number of UDP sessions originating from one source IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
udp_src_session	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
udp_dst_session	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
icmp_flood	If the number of ICMP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	250 packets per second.
icmp_sweep	If the number of ICMP packets originating from one source IP address exceeds the configured threshold value, the action is executed.	100 packets per second.
icmp_src_session	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.	300 concurrent sessions

Anomaly Name	Description	Recommended Threshold
icmp_dst_session	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.	3000 concurrent sessions
ip_src_session	If the number of concurrent IP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
ip_dst_session	If the number of concurrent IP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
sctp_flood	If the number of SCTP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second
sctp_scan	If the number of SCTP sessions originating from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second
sctp_src_session	If the number of concurrent SCTP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions
sctp_dst_session	If the number of concurrent SCTP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions

Status

The status field is enabled to enable the sensor for the associated anomaly. In terms of actions performed there is no difference between disabling a sensor and having the action as “Pass” but by disabling sensors that are not being used for blocking or logging you can save some resources of the firewall that can be better used elsewhere.

Logging

Regardless of whether the traffic is blocked or passed through the anomalous traffic will be logged.

Pass

Allows the anomalous traffic to pass through unimpeded.

Block

For Thresholds based on the number of concurrent sessions blocking the anomaly will not allow more than the number of concurrent sessions set as the threshold.

For rate based thresholds where the threshold is measured in packets per second, the Action setting “Block” prevents the overwhelming of the firewall by anomalous traffic in one of 2 ways. Setting which of those 2 ways will be issued is determined in the CLI.

- continuous - blocks any packets that match the anomaly criteria once the threshold has been reached
- periodical - allows matching anomalous traffic up to the rate set by the threshold.

If the period for a particular anomaly is 60 seconds, such as those where the threshold is measured in concurrent sessions, after the 60 second timer has expired, the number of allowed packets that match the anomaly criteria is reset to zero. This means that if you allow 10 sessions through before blocking, after the 60 seconds is up, another 10 will be allowed. The attrition of sessions from expiration should keep the allowed sessions from reaching the maximum.

To set the type of block action for the rate based anomaly sensors:

```
config ips global
   set anomaly-mode continuous
   set anomaly-mode periodical
end
```

Threshold

The threshold can be either in terms of concurrent session or in packets per second depending on which sensor is being referred to.

One-arm IDS

Interface-based policy only defines what and how IPS functions are applied to the packets transmitted by the interface. It works no matter if the port is used in a forwarding path or used as an One-Arm device.

To enable One-Arm IDS, the user should first enable sniff-mode on the interface,

```
config system interface
   edit port2
      set ips-sniffer-mode enable
   next
end
```

Once sniff-mode is turned on, both incoming and outgoing packets will be dropped after IPS inspections. The port can be connected to a hub or a switch's SPAN port. Any packet picked up by the interface will still follow the interface policy so different IPS and DoS anomaly checks can be applied.

IPv6 IPS

IPv6 IPS signature scan can be enabled by interface policy. The user can create an normal IPS sensor and assign it to the IPv6 interface policy.

```
config firewall interface-policy6
   edit 1
      set interface "port1"
      set srcaddr6 "all"
      set dstaddr6 "all"
      set service6 "ANY"
      set ips-sensor-status enable
      set ips-sensor "all_default"
   next
end
```

Traffic destined to the FortiGate unit

IPS enabled in firewall policies can only inspect the traffic pass through FortiGate unit, not the traffic destined to FortiGate unit. Enabling IPS in interface-policy allows IPS to pick up any packet on the interface so it is able to inspect attacks targeting FGT.

Dropped, flooded, broadcast, multicast and L2 packets

In many evaluation or certification tests, FortiGate firewall is often required to log any packets dropped by the firewall. In most of cases, these packets are of invalid headers so firewall just drops them silently. It is natural to forward all these packets to IPS first so FortiGate firewall is able to generate logs for invalid packets.

Flooded, broadcast and multicast traffics do not reach any of services in the forwarding path. They can be inspected by the interface policy as long as they match the addresses defined. Potentially, L2 packets can also be sent to IPS for inspection through interface-policy, but it is not enabled in FortiOS 5.2.

GUI and CLI

Now in FortiGate, there are two places that IPS can be enabled, in a firewall policy and in an interface policy. In the firewall policy implementation, IPS sensor can be configured in both CLI and GUI. When adding an IPS sensor to an interface policy it must be done through the CLI. There is no GUI input window for the “Interface Policy”. There is however, a DoS Policy section in the GUI.

Local-In policies

On the FortiGate unit, there are a number of protocols and traffic that is specific to the internal workings of FortiOS. For many of these traffic sources, you can identify a specific port/IP address for this self-originating traffic. The following traffic can be configured to a specific port/IP address:

- SNMP
- Syslog
- alert email
- FortiManager connection IP
- FortiGuard services
- FortiAnalyzer logging
- NTP
- DNS
- Authorization requests such as RADIUS
- FSSO

Security policies control the flow of traffic through the FortiGate unit. The FortiGate unit also includes the option of controlling internal traffic, that is, management traffic.

Each interface includes an allow access configuration to allow management access for specific protocols. Local policies are set up automatically to allow all users all access. Local-in policies takes this a step further, to enable or restrict the user with that access. This also extends beyond the allow access selection.

Local-in policies are configured in the CLI with the commands:

```
config firewall local-in-policy
   edit <policy_number>
      set intf <source_interface>
      set srcaddr <source_address>
```

```
      set dstaddr <destination_address>
      set action {accept | deny}
      set service <service name>
      set schedule <schedule_name>
   end
```

For example, you can configure a local-in policy so that only administrators can access the FortiGate unit on weekends from a specific management computer at 192.168.21.12, represented by the address object mgmt-comp1, using SSH on port 3 (192.168.21.77 represented by the address object FG-port3) using the Weekend schedule which defines the time the of access.

```
config firewall local-in-policy
   edit <1>
      set intf port3
      set srcaddr mgmt-comp1
      set dstaddr FG-port3
      set action accept
      set service SSH
      set schedule Weekend
   end
```

You can also disable a policy should there be a requirement to turn off a policy for troubleshooting or other purpose. To disable a policy enter the commands:

```
config firewall local-in-policy
   edit <policy_number>
      set status disable
   end
```

Use the same commands with a status of enable to use the policy again.

Local-in policies are also supported for IPv6 by entering the command

```
config firewall local-in-policy6.
```

Security policy 0

Any security policy that is automatically added by the FortiGate unit has a policy ID number of zero (0). The most common reasons the FortiGate unit creates this policy is:

- The IPsec policy for FortiAnalyzer (and FortiManager version 3.0) is automatically added when an IPsec connection to the FortiAnalyzer unit or FortiManager is enabled.
- The policy to allow FortiGuard servers to be automatically added has a policy ID number of zero.
- The (default) drop rule that is the last rule in the policy and that is automatically added has a policy ID number of zero.
- When a network zone is defined within a VDOM, the intra-zone traffic set to allow or block is managed by policy 0 if it is not processed by a configured security policy.

This policy can appear in logs but will never appear in the security policy list, and therefore, can never be repositioned in the list.

When viewing the FortiGate firewall logs, you may find a log field entry indicating policyid=0. The following log message example indicates the log field policyid=0 in bold.

```
2008-10-06 00:13:49 log_id=0022013001 type=traffic subtype=violation pri=warning
    vd=root SN=179089 duration=0 user=N/A group=N/A rule=0 policyid=0 proto=17
    service=137/udp app_type=N/A status=deny src=10.181.77.73 srcname=10.181.77.73
    dst=10.128.1.161 dstname=10.128.1.161 src_int=N/A dst_int="Internal" sent=0 rcvd=0
    src_port=137 dst_port=137 vpn=N/A tran_ip=0.0.0.0 tran_port=0
```

Deny policies

Deny security policies deny traffic that is coming into the network. The FortiGate unit automatically blocks traffic that is associated with a deny security policy.

Deny security policies are usually configured when you need to restrict specific traffic, for example, SSH traffic. Deny security policies can also help when you want to block a service, such as DNS, but allow a specific DNS server.

There is a disparity in the effectiveness of deny policies. Only deny policies that contain VIPs will block traffic directed at those VIPs. Policies with VIPs are processed before other polices, so using a deny policy earlier in the list will not work. For more on this topic, read the "Exception to policy order" on page 1009.

Accept policies

Accept security policies accept traffic that is coming into the network. These policies allow traffic through the FortiGate unit, where the packets are scanned, translated if NAT is enabled, and then sent out to its destination.

Accept security policies are the most common security policies that are created in FortiOS. These security policies are basic policies, such as allowing Internet access, as well as complex policies, such as IPsec VPN.

Fixed port

Some network configurations do not operate correctly if a NAT policy translates the source port of packets used by the connection. NAT translates source ports to keep track of connections for a particular service.

From the CLI you can enable fixedport when configuring a security policy for NAT policies to prevent source port translation.

```
config firewall policy
   edit <policy-id>
      ...
      set fixedport enable
      ...
   end
```

However, enabling fixedport means that only one connection can be supported through the firewall for this service. To be able to support multiple connections, add an IP pool, and then select Dynamic IP pool in the policy. The firewall randomly selects an IP address from the IP pool and assigns it to each connection. In this case, the number of connections that the firewall can support is limited by the number of IP addresses in the IP pool.

Endpoint security

Endpoint security enforces the use of the FortiClient End Point Security (FortiClient and FortiClient Lite) application on your network. It can also allow or deny endpoints access to the network based on the application installed on them.

By applying endpoint security to a security policy, you can enforce this type of security on your network. FortiClient enforcement can check that the endpoint is running the most recent version of the FortiClient application, that the antivirus signatures are up-to-date, and that the firewall is enabled. An endpoint is usually often a single PC with a single IP address being used to access network services through a FortiGate unit.

With endpoint security enabled on a policy, traffic that attempts to pass through, the FortiGate unit runs compliance checks on the originating host on the source interface. Non-compliant endpoints are blocked. If someone is browsing the web, the endpoints are redirected to a web portal which explains the non-compliance and provides a link to download the FortiClient application installer. The web portal is already installed on the FortiGate unit, as a replacement message, which you can modify if required.

Endpoint Security requires that all hosts using the security policy have the FortiClient Endpoint Security agent installed. Currently, FortiClient Endpoint Security is available for Microsoft Windows 2000 and later only.

For more information about endpoint security, see the Security Profiles chapter in the FortiOS Handbook.

Traffic logging

When you enable logging on a security policy, the FortiGate unit records the scanning process activity that occurs, as well as whether the FortiGate unit allowed or denied the traffic according to the rules stated in the security policy. This information can provide insight into whether a security policy is working properly, as well as if there needs to be any modifications to the security policy, such as adding traffic shaping for better traffic performance.

Depending on what the FortiGate unit has in the way of resourses, there may be advantages in optimizing the amount of logging taking places. This is why in each policy you are given 3 options for the logging:

- **No Log** - Does not record any log messages about traffic accepted by this policy.
- **Log Security Events** - records only log messages relating to security events caused by traffic accepted by this policy.
- **Log all Sessions** - records all log messages relating to all of the traffic accepted by this policy.

  Depending on the the model, if the Log all Sessions option is selected there may be 2 additional options. These options are normally available in the GUI on the higher end models such as the FortiGate 600C or larger.
  - **Generate Logs when Session Starts**
  - **Capture Packets**

You can also use the CLI to enter the following command to write a log message when a session starts:

```
config firewall policy
   edit <policy-index>
      set logtraffic-start
   end
```

Traffic is logged in the traffic log file and provides detailed information that you may not think you need, but do. For example, the traffic log can have information about an application used (web: HTTP.Image), and whether or not the packet was SNAT or DNAT translated. The following is an example of a traffic log message.

```
2011-04-13
05:23:47
log_id=4
type=traffic
subtype=other
pri=notice
vd=root
status="start"
src="10.41.101.20"
srcname="10.41.101.20"
src_port=58115
dst="172.20.120.100"
dstname="172.20.120.100"
```

```
dst_country="N/A"
dst_port=137
tran_ip="N/A"
tran_port=0
tran_sip="10.31.101.41"
tran_sport=58115
service="137/udp"
proto=17
app_type="N/A"
duration=0
rule=1
policyid=1
sent=0
rcvd=0
shaper_drop_sent=0
shaper_drop_rcvd=0
perip_drop=0
src_int="internal"
dst_int="wan1"
SN=97404 app="N/A"
app_cat="N/A"
carrier_ep="N/A"
```

If you want to know more about logging, see the Logging and Reporting chapter in the FortiOS Handbook. If you want to know more about traffic log messages, see the FortiGate Log Message Reference.

Quality of service

The Quality of Service (QoS) feature allows the management of the level of service and preference given to the various types and sources of traffic going through the firewall so that the traffic that is important to the services and functions connecting through the firewall gets the treatment required to ensure the level of quality that is required.

QoS uses the following techniques:

Traffic policing	Packets are dropped that do not conform to bandwidth limitations
Traffic Shaping	Assigning minimum levels of bandwidth to be allocated to specific traffic flows to guarantee levels of servers or assigning maximum levels of bandwidth to be allocated to specific traffic flows so that they do not impede other flows of traffic.

This helps to ensure that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Traffic shaping also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instant in time. Flows that are greater than the maximum rate are subject to traffic policing.

Queuing

Assigning differing levels priority to different traffic flows so that traffic flows that are adversely effected by latency are prevented from being effected by traffic flows that are not subject to the effects of latency. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.

An example of where you would want to use something like this is if you had competing traffic flows of Voice over IP traffic and email traffic. The VoIP traffic is highly susceptible to latency issues.If you have a delay of a few seconds it is quickly noticeable when it is occurring. Email on the other hand can have a time delay of much longer and it is highly unlikely that it will be noticed at all.

By default, the priority given to any traffic is high, so if you want to give one type of traffic priority over all other traffic you will need to lower the priority of all of the other traffic.

Policy Monitor

Once policies have been configured and enabled it is useful to be able to monitor them. To get an overview about what sort of traffic the policies are processing go to Policy > Monitor > Policy Monitor.

The window is separated into two panes.

Upper pane

The upper pane displays a horizontal bar graph comparing the **Top Policy Usage** based on one of the following criteria:

- Active Sessions
- Bytes
- Packets

The criteria that the displayed graph is based on can be selected from the drop down menu in the upper right corner of the pane. The field name is **Report By:**.

The bars of the graph are interactive to an extent and can be used to drill down for more specific information. If you hover the cursor over the bar of the graph a small popup box will appear displaying more detailed information. If the bar of the graph is selected an entirely new window will be displayed using a vertical bar graph to divide the data that made up the first graph by IP address.

For example if the first graph was reporting usage by active sessions it would include a bar for each of the top policies with a number at the end showing how many sessions were currently going through that policy. If one of the bars of the graph was then selected the new bar graph would show the traffic of that policy separated by either **Source Address**, **Destination Address** or **Destination Port**. As in the other window, the selection for the reported criteria is in the upper right corner of the pane. If the parameter was by source address there would be a bar for each of the IP addresses sending a session through the policy and the end of the bar would show how many sessions.

To go back to the previous window of information in the graphs select the Return link in the upper left of the pane.

Lower pane

The lower pane contains a spreadsheet of the information that the bar graph will derive their information from. The column headings will include:

- Policy ID
- Source Interface/Zone
- Destination Interface/Zone
- Action

- Active Sessions
- Bytes
- Packets

Network defense

This section describes in general terms the means by which attackers can attempt to compromise your network and steps you can take to protect it. The goal of an attack can be as complex as gaining access to your network and the privileged information it contains, or as simple as preventing customers from accessing your web server. Even allowing a virus onto your network can cause damage, so you need to protect against viruses and malware even if they are not specifically targeted at your network.

The following topics are included in this section:

- Monitoring
- Blocking external probes
- Defending against DoS attacks

Monitoring

Monitoring, in the form of logging, alert email, and SNMP, does not directly protect your network. But monitoring allows you to review the progress of an attack, whether afterwards or while in progress. How the attack unfolds may reveal weaknesses in your preparations. The packet archive and sniffer policy logs can reveal more details about the attack. Depending on the detail in your logs, you may be able to determine the attackers location and identity.

While log information is valuable, you must balance the log information with the resources required to collect and store it.

Blocking external probes

Protection against attacks is important, but attackers often use vulnerabilities and network tools to gather information about your network to plan an attack. It is often easier to prevent an attacker from learning important details about your network than to defend against an attack designed to exploit your particular network.

Attacks are often tailored to the hardware or operating system of the target, so reconnaissance is often the first step. The IP addresses of the hosts, the open ports, and the operating systems the hosts are running is invaluable information to an attacker. Probing your network can be as simple as an attacker performing an address sweep or port scan to a more involved operation like sending TCP packets with invalid combinations of flags to see how your firewall reacts.

Address sweeps

An address sweep is a basic network scanning technique to determine which addresses in an address range have active hosts. A typical address sweep involves sending an ICMP ECHO request (a ping) to each address in an address range to attempt to get a response. A response signifies that there is a host at this address that responded to the ping. It then becomes a target for more detailed and potentially invasive attacks.

Address sweeps do not always reveal all the hosts in an address range because some systems may be configured to ignore ECHO requests and not respond, and some firewalls and gateways may be configured to prevent ECHO requests from being transmitted to the destination network. Despite this shortcoming, Address sweeps are still used because they are simple to perform with software tools that automate the process.

Use the `icmp_sweep` anomaly in a DoS policy to protect against address sweeps.

There are a number of IPS signatures to detect the use of ICMP probes that can gather information about your network. These signatures include `AddressMask, Traceroute, ICMP.Invalid.Packet.Size`, and `ICMP.Oversized.Packet`. Include ICMP protocol signatures in your IPS sensors to protect against these probes/attacks.

Port scans

Potential attackers may run a port scan on one or more of your hosts. This involves trying to establish a communication session to each port on a host. If the connection is successful, a service may be available that the attacker can exploit.

Use the DoS anomaly check for `tcp_port_scan` to limit the number of sessions (complete and incomplete) from a single source IP address to the configured threshold. If the number of sessions exceed the threshold, the configured action is taken.

Use the DoS anomaly check for `udp_scan` to limit UDP sessions in the same way.

Probes using IP traffic options

Every TCP packet has space reserved for eight flags or control bits. They are used for communicating various control messages. Although space in the packet is reserved for all eight, there are various combinations of flags that should never happen in normal network operation. For example, the SYN flag, used to initiate a session, and the FIN flag, used to end a session, should never be set in the same packet.

Attackers may create packets with these invalid combinations to test how a host will react. Various operating systems and hardware react in different ways, giving a potential attackers clues about the components of your network.

The IPS signature `TCP.Bad.Flags` detects these invalid combinations. The default action is pass though you can override the default and set it to **Block** in your IPS sensor.

Configure packet replay and TCP sequence checking

The anti-replay CLI command allows you to set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SEQ) number checking). All TCP packets contain a Sequence Number (SEQ) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets.

FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

Configure the anti-replay CLI command:

```
config system global
   set anti-replay {disable | loose | strict}
end
```

You can set anti-replay protection to the following settings:

- `disable` — No anti-replay protection.
- `loose` — Perform packet sequence checking and ICMP anti-replay checking with the following criteria:
- The SYN, FIN, and RST bit can not appear in the same packet.

- The FortiGate unit does not allow more than one ICMP error packet through before it receives a normal TCP or UDP packet.
- If the FortiGate unit receives an RST packet, and check-reset-range is set to strict, the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
- `strict` — Performs all of the loose checking but for each new session also checks to determine of the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.

If any packet fails a check it is dropped.

Configure ICMP error message verification

Enable ICMP error message verification to ensure an attacker can not send an invalid ICMP error message.

```
config system global
   check-reset-range {disable | strict}
end
```

- `disable` — the FortiGate unit does not validate ICMP error messages.
- `strict` — enable ICMP error message checking.

If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. Strict checking also affects how the anti-replay option checks packets.

Protocol header checking

Select the level of checking performed on protocol headers.

```
config system global
   check-protocol-header {loose | strict}
end
```

- `loose` — the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc.
- `strict` — the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length.

If the packet fails header checking it is dropped by the FortiGate unit.

Evasion techniques

Attackers employ a wide range of tactics to try to disguise their techniques. If an attacker disguises a known attack in such a way that it is not recognized, the attack will evade your security and possibly succeed. FortiGate security recognizes a wide variety of evasion techniques and normalizes data traffic before inspecting it.

Packet fragmentation

Information sent across local networks and the Internet is encapsulated in packets. There is a maximum allowable size for packets and this maximum size varies depending on network configuration and equipment limitations. If a packet arrives at a switch or gateway and it is too large, the data it carries is divided among two or more smaller packets before being forwarded. This is called fragmentation.

When fragmented packets arrive at their destination, they are reassembled and read. If the fragments do not arrive together, they must be held until all of the fragments arrive. Reassembly of a packet requires all of the fragments.

The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. This reassembly of packets affects TCP, UDP and IP packets. There can be some variation though in what process does the reassembling. The IPS engine, nTurbo and the kernel all can do defragmentation.

For example, you have configured the FortiGate unit to block access to the example.org web site. Any checks for example.com will fail if a fragmented packet arrives and one fragment contains `http://www.exa` while the other contains `mple.com/`. Viruses and malware can be fragmented and avoid detection in the same way. The FortiGate unit will reassemble fragmented packets before examining network data to ensure that inadvertent or deliberate packet fragmentation does not hide threats in network traffic.

Non-standard ports

Most traffic is sent on a standard port based on the traffic type. The FortiGate unit recognizes most traffic by packet content rather than the TCP/UDP port and uses the proper IPS signatures to examine it. Protocols recognized regardless of port include DHCP, DNP3, FTP, HTTP, IMAP, MS RPC, NNTP, POP3, RSTP, SIP, SMTP, and SSL, as well as the supported IM/P2P application protocols.

In this way, the FortiGate unit will recognize HTTP traffic being sent on port 25 as HTTP rather than SMTP, for example. Because the protocol is correctly identified, the FortiGate unit will examine the traffic for any enabled HTTP signatures.

Negotiation codes

Telnet and FTP servers and clients support the use of negotiation information to allow the server to report what features it supports. This information has been used to exploit vulnerable servers. To avoid this problem, the FortiGate unit removes negotiation codes before IPS inspection.

HTTP URL obfuscation

Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser.

The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection.

HTTP URL obfuscation types

Encoding type	Example
No encoding	http://www.example.com/cgi.bin/
Decimal encoding	http://www.example.com/cgi.bin/
URL encoding	http://www.example.com/%43%47%49%2E%42%49%4E%2F
ANSI encoding	http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0069%u006E/
Directory traversal	http://www.example.com/cgi.bin/test/../

HTTP header obfuscation

The headers of HTTP requests or responses can be modified to make the discovery of patterns and attacks more difficult. To prevent this, the FortiGate unit will:

- remove junk header lines
- reassemble an HTTP header that's been folded onto multiple lines
- move request parameters to HTTP POST body from the URL

The message is scanned for any enabled HTTP IPS signatures once these problems are corrected.

HTTP body obfuscation

The body content of HTTP traffic can be hidden in an attempt to circumvent security scanning. HTTP content can be GZipped or deflated to prevent security inspection. The FortiGate unit will uncompress the traffic before inspecting it.

Another way to hide the contents of HTTP traffic is to send the HTTP body in small pieces, splitting signature matches across two separate pieces of the HTTP body. The FortiGate unit reassembles these 'chunked bodies' before inspection.

Microsoft RPC evasion

Because of its complexity, the Microsoft Remote Procedure Call protocol suite is subject to a number of known evasion techniques, including:

- SMB-level fragmentation
- DCERPC-level fragmentation
- DCERPC multi-part fragmentation
- DCERPC UDP fragmentation
- Multiple DCERPC fragments in one packet

The FortiGate unit reassembles the fragments into their original form before inspection.

Defending against DoS attacks

A denial of service is the result of an attacker sending an abnormally large amount of network traffic to a target system. Having to deal with the traffic flood slows down or disables the target system so that legitimate users can not use it for the duration of the attack.

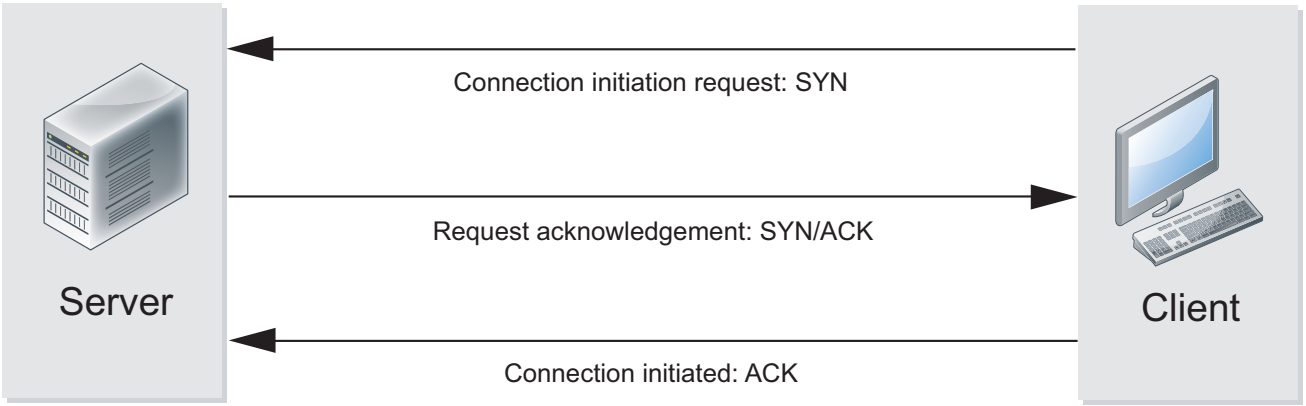
Any network traffic the target system receives has to be examined, and then accepted or rejected. TCP, UDP, and ICMP traffic is most commonly used, but a particular type of TCP traffic is the most effective. TCP packets with the SYN flag are the most efficient DoS attack tool because of how communication sessions are started between systems.

The “three-way handshake”

Communication sessions between systems start with establishing a TCP/IP connection. This is a simple three step process, sometimes called a “three-way handshake,” initiated by the client attempting to open the connection.

1. The client sends a TCP packet with the SYN flag set. With the SYN packet, the client informs the server of its intention to establish a connection.
2. If the server is able to accept the connection to the client, it sends a packet with the SYN and the ACK flags set. This simultaneously acknowledges the SYN packet the server has received, and informs the client that the server intends to establish a connection.
3. To acknowledge receipt of the packet and establish the connection, the client sends an ACK packet.

Establishing a TCP/IP connection



The three-way handshake is a simple way for the server and client to each agree to establish a connection and acknowledge the other party expressing its intent. Unfortunately, the three-way handshake can be used to interfere with communication rather than facilitate it.

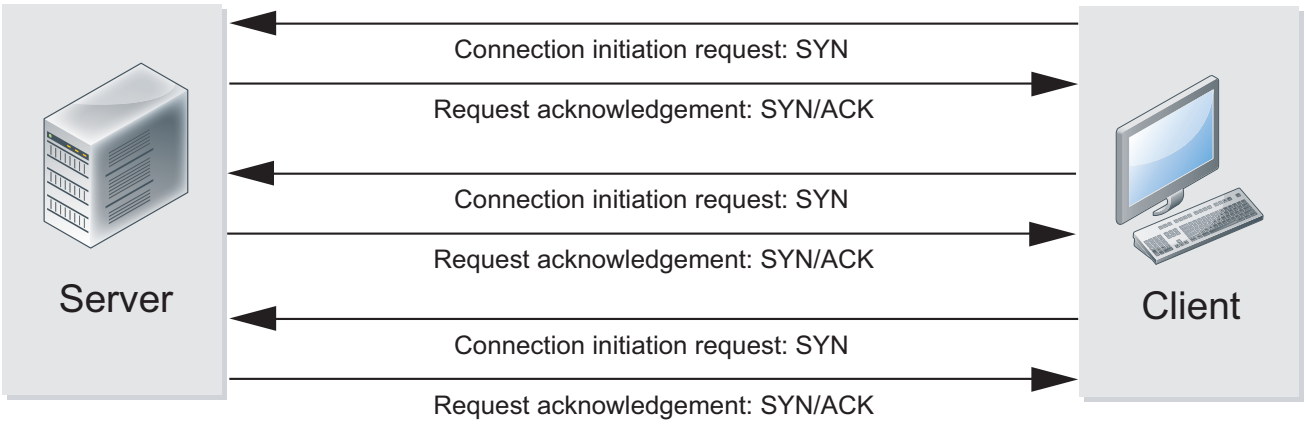
SYN flood

When a client sends a SYN packet to a server, the server creates an entry in its session table to keep track of the connection. The server then sends a SYN+ACK packet expecting an ACK reply and the establishment of a connection.

An attacker intending to disrupt a server with a denial of service (DoS) attack can send a flood of SYN packets and not respond to the SYN+ACK packets the server sends in response. Networks can be slow and packets can get lost so the server will continue to send SYN+ACK packets until it gives up, and removes the failed session from

the session table. If an attacker sends enough SYN packets to the server, the session table will fill completely, and further connection attempts will be denied until the incomplete sessions time out. Until this happens, the server is unavailable to service legitimate connection requests.

A single client launches a SYN flood attack

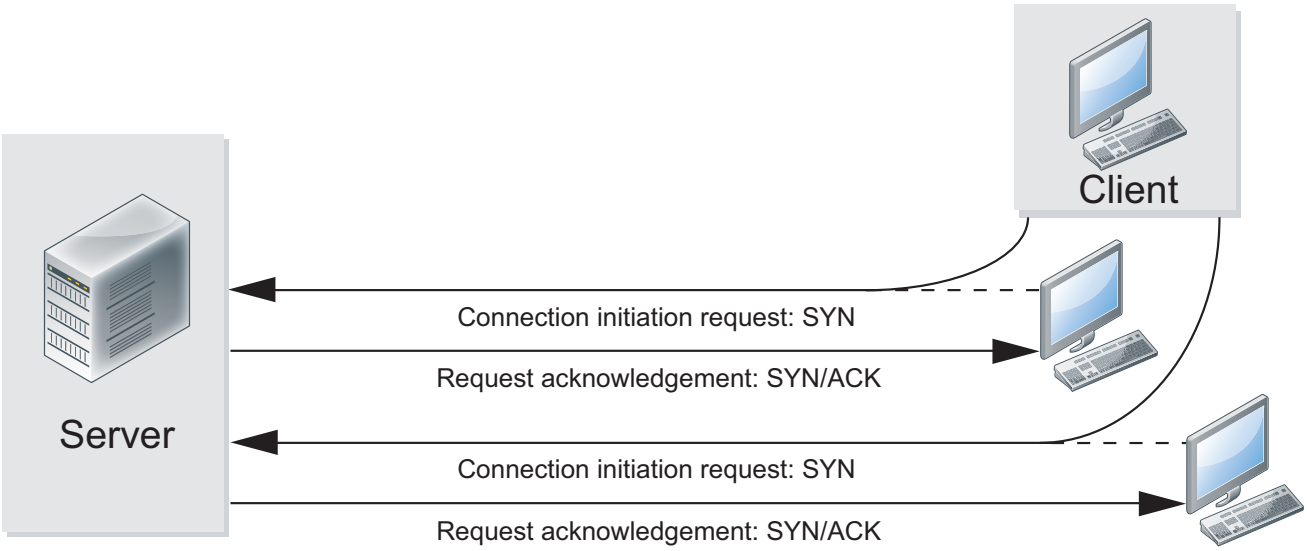


SYN floods are seldom launched from a single address so limiting the number of connection attempts from a single IP address is not usually effective.

SYN spoofing

With a flood of SYN packets coming from a single attacker, you can limit the number of connection attempts from the source IP address or block the attacker entirely. To prevent this simple defense from working, or to disguise the source of the attack, the attacker may spoof the source address and use a number of IP addresses to give the appearance of a distributed denial of service (DDoS) attack. When the server receives the spoofed SYN packets, the SYN+ACK replies will go to the spoofed source IP addresses which will either be invalid, or the system receiving the reply will not know what to do with it.

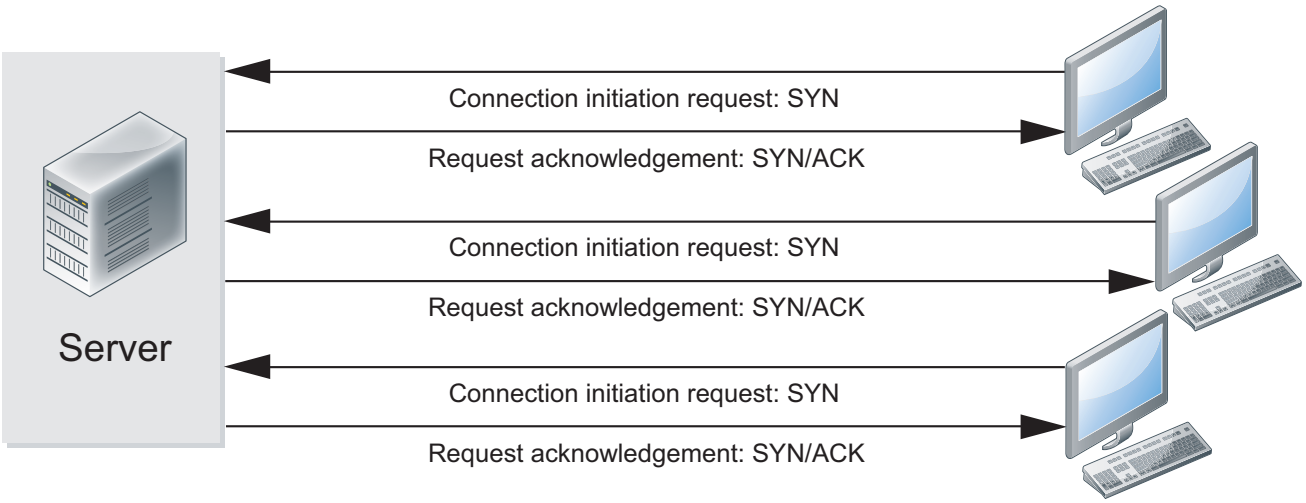
A client launches a SYN spoof attack



DDoS SYN flood

The most severe form of SYN attack is the distributed SYN flood, one variety of distributed denial of service attack (DDoS). Like the SYN flood, the target receives a flood of SYN packets and the ACK+SYN replies are never answered. The attack is distributed across multiple sources sending SYN packets in a coordinated attack.

Multiple attackers launch a distributed SYN flood



The distributed SYN flood is more difficult to defend against because multiple clients are capable of creating a larger volume of SYN packets than a single client. Even if the server can cope, the volume of traffic may overwhelm a point in the network upstream of the targeted server. The only defence against this is more bandwidth to prevent any choke-points.

Configuring the SYN threshold to prevent SYN floods

The preferred primary defence against any type of SYN flood is the DoS anomaly check for `tcp_syn_flood` threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to **Pass**, the FortiGate unit will allow the SYN packets that exceed the threshold. If the action is set to **Block**, the FortiGate unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.

The tools attackers use to generate network traffic will not send a second SYN packet when a SYN+ACK response is not received from the server. These tools will not “retry.” Legitimate clients will retry when no response is received, and these retries are allowed even if they exceed the threshold with the action set to **Block**.

SYN proxy

FortiGate units with network acceleration hardware, whether built-in or installed in the form of an add-on module, offer a third action for the `tcp_syn_flood` threshold. Instead of **Block** and **Pass**, you can choose to **Proxy** the incomplete connections that exceed the threshold value.

When the `tcp_syn_flood` threshold action is set to **f**, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the FortiGate unit receives an ACK response as expected, it will “replay” this exchange to the server to establish a communication session between the client and the server, and allow the communication to proceed.

Other flood types

UDP and ICMP packets can also be used for DoS attacks, though they are less common. TCP SYN packets are so effective because the target receives them and maintains a session table entry for each until they time out. Attacks using UDP or ICMP packets do not require the same level of attention from a target, rendering them less effective. The target will usually drop the offending packets immediately, closing the session.

Use the `udp_flood` and `icmp_flood` thresholds to defend against these DoS attacks.

DoS policies

DDoS attacks vary in nature and intensity. Attacks aimed at saturating the available bandwidth upstream of your service can only be countered by adding more bandwidth. DoS policies can help protect against DDoS attacks that aim to overwhelm your server resources.

DoS policy recommendations

- Use and configure DoS policies to appropriate levels based on your network traffic and topology. This will help drop traffic if an abnormal amount is received.
- It is important to set a good threshold. The threshold defines the maximum number of sessions/packets per second of normal traffic. If the threshold is exceeded, the action is triggered. Threshold defaults are general recommendations, although your network may require very different values.
- One way to find the correct values for your environment is to set the action to **Pass** and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your system will be from DoS attacks, but your system will also be more likely to generate false alarms.

GUI and CLI - what you may not know

The Graphic User Interface (GUI) is designed to be as intuitive as possible but there are always a few things that are left out because to put all of that information on the interface would clutter it up to the point where it wouldn't be graphical and intuitive anymore.

This section is made up of knowledge that will make working with the both of the management interfaces easier because you wont have to find out about things like field limitations through trial and error. Some of it has to do with changing in how navigation in the GUI has changed.

The section includes the topics:

- Mouse Tricks
- Changing the default column setting on the policy page
- Naming Rules and Restrictions
- Character Restrictions
- Length of Fields Restrictions
- Object Tagging and Coloring
- Numeric Values
- Selecting options from a list
- Enabling or disabling options
- To Enable or Disable Optionally Displayed Features

Mouse tricks

In previous version of the firmware much of the navigation, editing or choosing of options in the Web-based Manager was carried out by using the mouse in combination with a number of icons visible on the interface. This version of the firmware makes more extensive use of the right or secondary mouse button as well as the “drag and drop” feature. If you are used to the old Web-based Manager interface you will notice that a number of the options at the top of the display window are not there anymore or there are fewer of them.

To get a feel for the new approach the **Policy & Objects > Policy > IPv4** window is a noticeable place to see some of these changes in action.

The different view modes are still in the upper right-hand corner as they were before but now there is no column settings link to move or configure the columns of the window. Now if you wish to reposition a column just use the mouse to click on the column heading and drag it to its new position. If you wish to add a new column just right-click on one of the column headings and a drop down menu will appear with the option “Column Settings”. Use the right pointing triangle to expand the “Column Settings” option to see a choice of possible columns for the window you are in. Those already selected will be at the top with a checked box and the available new ones will be at the bottom ready to be selected.

Rather than having a link to initiate a move in the positioning of policies in the sequence, you can select a policy and hold down the mouse button and drag it to its new position.

By right or secondary clicking the mouse curser in the cells of the Policy window you will get a drop down menu that is contextual to the column and policy row where you made the clck.For example if you right click in the “Schedule” column for the row that is for policy #5 you will get the option to select a schedule for policy #5 along with a number of other configuration options relating to that policy or its position in the sequence of policies.

You will find this approach used much more frequently through out the Web-based Manager, giving it a more modern and intuitive feel once you learn to use the right mouse button rather than finding a link displayed on the page.

Changing the default column setting on the policy page

The **Policy & Objects > Policy > IPv4** window is one of the more important ones in the Web based interface and has the capacity to display a lot of information, but displaying all of that information at the same time makes for a very busy screen. If all of the columns are displayed, depending on the screen size you may have to constantly use the scroll bars to see what you need to look at. The default installation shows some of the more commonly used columns but these list may not consist of the columns that you wish to look at or the order that you wish to view them in. For this reason it is possible, through the CLI to override these settings to establish a new default.

The syntax of the command starts with:

```
config system settings
   set gui-default-policy-columns
```

The rest of the command is a space delimited list that depends on the columns you wish to view and the order you wish to view them in. The possible selection is in the following table.

Variables for the gui-default-policy-columns command

Variable Name	Column Heading
#	Sequence Number
policyid	Policy ID
srcintf	Source Interface
dstintf	Destination Interface
srcaddr	Source Addresses
dstaddr	Destination Addresses
schedule	Policy Schedule
service	Policy Services
action	Policy Action
logtraffic	Traffic Logging Status
nat	Policy NAT Status
status	Policy Status
authentication	Authentication Groups
count	Policy Traffic Counter
profile	Security Profiles
vpntunnel	VPN Tunnel
comments	Policy Comment

Example

If you wanted these columns in this order, Policy ID, Source Addresses, Destination Addresses, Security Profiles, Policy Comment. You would enter the command:

```
config system settings
   set gui-default-policy-columns policyid srcaddr dstaddr profile comments
```

Naming rules and restrictions

The following are the specific rules that are obeyed by the FortiGate.

Duplicate Name Issues:

- A VLAN cannot have the same name as a physical interface.
- An Address must not have the same name as an Address Group.
- An Address or Address Group must not have the same name as a Virtual IP Address.
- A Service cannot have the same name as a Service Group.
- A VLAN must not have the same name as a VDOM.
- A VLAN or VDOM must not have the same name as a Zone.

Try to make each firewall object name as unique as possible so that it cannot be confused with another object.

Character restrictions

Object names cannot contain the following characters:

- <
- >
- (
-)

All other characters, including other languages, are supported as usable characters.

> FortiOS allows spaces in just about all object name fields, but this was not always the case. Some people are still cautious where this is concerned. If you're cautious about characters in the names of objects use this basic rule of thumb:
>
> When naming objects, only use characters that are alphanumeric (a-z, A-Z, 0-9) and where there is the temptation to use spaces in a name, use the '-' (dash) and '_' (underscore).

Numeric values

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Numeric values

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Selecting options from a list

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

Enabling or disabling options

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

To enable or disable optionally displayed features

There are a number of features in the web-based manager that can be configured to either be displayed if you are likely to use them or disabled if you have no need to see them. The ones that may be relevant to the function of the Firewall are:

- Central NAT Table
- Dynamic Profile
- Explicit Proxy
- Implicit Firewall Policies
- IPv6
- Load Balance
- Local In Policy

You can enable or disable these features by going to **System > Admin > Settings** or by using the following CLI options:

```
config system global
   set gui-ap-profile {disable | enable}
   set gui-central-nat-table {disable | enable}
   set gui-dns-database {disable | enable}
   set gui-dynamic-profile-display {disable | enable}
   set gui-icap {disable | enable}
   set gui-implicit-id-based-policy {disable | enable}
   set gui-implicit-policy {disable | enable}
   set gui-ipsec-manual-key {enable | disable}
   set gui-ipv6 {enable | disable}
   set gui-lines-per-page <gui_lines>
   set gui-load-balance {disable | enable}
   set gui-object-tags {disable | enable}
   set gui-policy-interface-pairs-view {enable | disable}
   set gui-voip-profile {disable | enable}
end
```

Building firewall objects and policies

The other chapters in the Firewall book have so far been concerned primarily with concepts and abstract ideas that are designed you help you understand what is going on with the firewall and what it can do. Now that we have a good grounding in the “what” it is time to get into the “how”.

This section will provide the instructions for the web-based manager (when available) and the CLI for adding and or editing FortiGate firewall objects and then how to put them together when building a policy to govern the traffic flowing through your network. To give some context, scenarios have been included. The instructions here are concerned with the creation of the objects. The inclusion of these objects into firewall policies is not shown in these instructions.

This chapter includes the instructions for building the following:

- IPv4 Firewall Addresses
- IPv6 Firewall Addresses
- FQDN address

- Changing the TTL of a FQDN address
- New Geography-based Address
- IPv4 Address Group
- IPv4 Address Group
- IPv6 Address Group
- Multicast Address
- Service Category
- TCP/UDP/SCTP Service
- ICMP Service
- ICMPv6 Service
- Service Group
- Virtual IP address
- IP Pool
- Central NAT Table
- Firewall Schedule - Recurring
- Firewall Schedule - One-time
- Schedule Group
- Proxy Option
- DoS Policy

Building firewall objects and policies

The other chapters in the Firewall book have so far been concerned primarily with concepts and abstract ideas that are designed you help you understand what is going on with the firewall and what it can do. Now that we have a good grounding in the “what” it is time to get into the “how”.

This section will provide the instructions for the web-based manager (when available) and the CLI for adding and or editing FortiGate firewall objects and then how to put them together when building a policy to govern the traffic flowing through your network. To give some context, scenarios have been included. The instructions here are concerned with the creation of the objects. The inclusion of these objects into firewall policies is not shown in these instructions.

This chapter includes the instructions for building the following:

- IPv4 Firewall Addresses
- IPv6 Firewall Addresses
- FQDN address
- Changing the TTL of a FQDN address
- New Geography-based Address
- IPv4 Address Group
- IPv4 Address Group
- IPv6 Address Group
- Multicast Address
- Service Category
- TCP/UDP/SCTP Service

- ICMP Service
- ICMPv6 Service
- Service Group
- Virtual IP address
- IP Pool
- Central NAT Table
- Firewall Schedule - Recurring
- Firewall Schedule - One-time
- Schedule Group
- Proxy Option
- DoS Policy

Example: IPv4 firewall addresses

Scenario: Mail server

You need to create an IPv4 address for the Mail Server on Port1 of your internal network.

- These server is on the network off of port1.
- The IP address is 192.168.1.27
- The subnet mask is 255.255.255.0
- There should be a tag for this address being for a server

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information:

Category	Address
Name	Mail_Server
Type	Subnet / IP Range
Subnet / IP Range	192.168.1.27/255.255.255.0
Interface	port1
Visibility	<enabled>
Comments	<add any additional discription>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address
   edit Mail_Server
      set type ipmask
      set subnet 192.168.1.27 255.255.255.255
      set associated-interface port1
   end
```

Scenario: First floor network

You need to create an IPv4 address for the subnet of the internal network off of Port1.

- These computers are on the network off of port1.
- The subnet is the range from 192.168.1.1 to 192.168.1.255.
- The subnet mask is 255.255.255.0
- There should be a reference to this being the network for the 1st floor of the building.

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	Address
Name	Internal_Subnet_1
Type	Subnet
Subnet / IP Range	192.168.1.0/24
Interface	port1
visibility	<enabled>
Comments	Network for 1st Floor

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address
   edit Internal_Subnet_1
      Set comment "Network for 1st Floor"
      set type ipmask
      set subnet 192.168.1.0/24
      set associated-interface port1
   end
```

Scenario: Marketing department

You need to create an IPv4 address for the address range for a group of computers used by the Marketing Department.

- These computers are on the network off of port1.
- The IP addresses for these computers range from 192.168.1.100 to 192.168.1.115

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	Address
Name	Marketing_computers
Type	IP Range

Subnet / IP Range	192.168.1.100-192.168.1.115
Interface	port1
Visibility	<enable>
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address
   edit Internal_Subnet_1
      set type iprange
      set start-ip 192.168.1.100
      set end-ip 192.168.1.115
      set associated-interface port1
   end
```

Verification

To verify that the addresses were added correctly:

1. Go to **Policy & Objects> Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall address
   edit <the name of the address to verify>
   show full-configuration
```

Example: IPv6 firewall addresses

Scenario: Mail server

You need to create an IPv6 address for the Mail Server on Port1 of your internal network.

- These server is on the network off of port1.
- The IP address is 2001:db8:0:2::20/64
- There should be a tag for this address being for a server

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	IPv6 Address
Name	Mail_Server
Type	Subnet
Subnet / IP Range	2001:db8:0:2::20/64
Interface	port1

Visibility	<enable>
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address6
   edit Mail_Server
      set type ipmask
      set subnet 2001:db8:0:2::20/64
      set associated-interface port1
   end
```

Scenario: First floor network

You need to create an IPv4 address for the subnet of the internal network off of Port1.

- These computers are on the network off of port1.
- The Network uses the IPv6 addresses: fdde:5a7d:f40b:2e9d:xxxx:xxxx:xxxx:xxxx
- There should be a reference to this being the network for the 1st floor of the building.

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	IPv6 Address
Name	Internal_Subnet_1
Type	Subnet
Subnet / IP Range	2001:db8:0:2::/64
Interface	port1
Visibility	<enable>
Comments	Network for 1st Floor

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address6
   edit Internal_Subnet_1
      Set comment "Network for 1st Floor"
      set subnet 2001:db8:0:2::/64
   end
```

Verification

To verify that the addresses were added correctly:

1. Go to **Policy & Objects> Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall address6
```

```
edit <the name of the address that you wish to verify>
   Show full-configuration
```

Example: FQDN address

You have to great a policy that will govern traffic that goes to a site that has a number of servers on the Internet. Depending on the traffic or the possibility that one of the servers is down network traffic can go to any one of those sites. The consistent factor is that they all use the same Fully Qualified Domain Name.

- The FQDN of the web site: example.com
- The number of ISP connections off of the FortiGate firewall: 2

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information:

Category	Address
Name	BigWebsite.com
Type	FQDN
FQDN	bigwebsite.com
Interface	any
Visibility	<enable>
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address
   edit BigWebsite.com
      set type fqdn
      set associated-interface any
      set fqdn bigwebsite.com
   end
```

Verification

To verify that the addresses were added correctly:

1. Go to **Firewall Objects > Address > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall address
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

Changing the TTL of a FQDN address

To make sure that the FQDN resolves to the most recent active server you have been asked to make sure that the FortiGate has not cached the address for any longer than 10 minutes.

There is no field for the cached time-to-live in the web-based manager. It is only configurable in the CLI. Enter the following commands:

```
config firewall address
   edit BigWebsite.com
      set cache-ttl 600
   end
```

Example: Geography-based address

Your company is US based and has information on its web site that may be considered information that is not allowed to be sent to embargoed countries. In an effort to help reduce the possibility of sensitive information going to those countries you have be asked to set up addresses for those countries so that they can be block in the firewall policies.

- One of the countries you have been asked to block is Cuba
- You have been asked to comment the addresses so that other administrators will know why they have been created

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	Address
Name	Cuba
Type	Geography
Country	Cuba
Interface	any
Visibility	<enable>
Comments	Embargoed

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address
   edit Cuba
      set type geography
      set country CN
      set interface wan1
   end
```

Example: IPv4 address group

Your company has a small division that is in Denmark that has a number of remote users that need to connect to a resource from either home, office or customer sites. The thing that they have in common is that there are all in Denmark. An address group needs to be created that will allow for this.

The preconfigured addresses to use will consist of:

- Denmark - a geography based address
- Denmark_ISP1 - a IP range of address of an ISP that services Denmark

- Denmark_ISP2 - a IP range of address of another ISP that services Denmark
- Denmark_Division - the FQDN of the Denmark office that uses Dynamic DNS

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address Group.**
2. Fill out the fields with the following information

Type	IPv4 Group
Group Name	Denmark_Users
Show in Address List	<enable>
Members	Denmark Denmark_ISP1 Denmark_ISP2 Denmark_Division
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall addrgrp
   edit Denmark_Users
      set member Denmark Denmark_ISP1 Denmark_ISP2 Denmark_Division
   end
```

To verify that the addresses were added correctly:

1. Go to **Policy & Objects> Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall addgrp
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

Example: IPv6 address group

Create IPv6 address groups from existing IPv6 addresses

Your company has 3 internal servers with IPv6 addresses that it would like to group together for the purposes of a number of policies.

The preconfigured addresses to use will consist of:

- Web_Server-1
- Web_Server-2
- Web_Server-3

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address Group.**
2. Fill out the fields with the following information

Type	IPv6 Group
Group Name	Web_Server_Cluster
Show in Address List	<enable>
Members	Web_Server-1 Web_Server-2 Web_Server-3
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall addrgrp6
   edit Web_Server_Cluster
      set member Web_Server-1 Web_Server-2 Web_Server-3
   end
```

To verify that the addresses were added correctly:

1. Go to **Policy & Objects> Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall addgrp6
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

Example: Multicast address

The company has a large high tech campus that has monitors in many of its meeting rooms. It is common practice for company wide notifications of importance to be done in a streaming video format with the CEO of the company addressing everyone at once.

The video is High Definition quality so takes up a lot of bandwidth. To minimize the impact on the network the network administrators have set things up to allow the use of multicasting to the monitors for these notifications. Now it has to be set up on the FortiGate firewall to allow the traffic.

- The range being used for the multicast is 239.5.0.0 to 239.5.255.255
- The interface on this FortiGate firewall will be on port 4

1. Go to **Policy & Objects> Objects > Addresses** and select **Create New > Address.**
2. Fill out the fields with the following information

Category	Multicast Address
Name	Meeting_Room_Displays
Type	Multicast IP Range

Multicast IP Range	239.5.0.0-239.5.255.255
Interface	port4
Visibility	<enable>
Comments	<Input into this field is optional>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall multicast-address
   edit "meeting_room_display"
      set associated-interface "port9"
      set start-ip 239.5.0.0
      set end-ip 239.5.255.255
      set visibility enable
      next
   end
```

To verify that the address range was added correctly:

1. Go to **Policy & Objects> Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall multicast-address
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

Example: Service category

Add a new category to the list of Service Categories

You plan on adding a number of devices such as web cameras that will allow the monitoring of the physical security of your datacenter. A number of non-standard services will have to be created and you would like to keep them grouped together under the heading of “Surveillance”

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Category.**
2. Fill out the fields with the following information

Name	Surveillance
Comments	For DataCenter Surveillance Devices

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service category
   Edit Surveillance
      Set comment “For DataCenter Surveillance Devices”
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services**. Select the Category Settings icon . A listing of the categories should be displayed.
2. Enter the following CLI command:

```
config firewall service category
  show
```

This should bring up all of the categories. Check to see that the new one is displayed.

Example: TCP/UDP/SCTP service

To create and configure a TCP/UDP/STCP protocol type service.

You have set up some new web cams at work that send a constant live feed to a security service. Not only do these cameras have a feed that can be sent offsite they can be remotely managed from a browser or an application.

The ports that need to be opened to use all of the features of the web cams are:

- Management by browser - TCP on port 8000
- Real time video feed - UDP on port 4000
- Connection through vendor application - SCTP on port 1600

The IP address of the offsite service is 256.25.56.12 (Not a valid IP address. Used for example only)

- One service will be needed for the incoming connections
- One service will be needed for the outgoing connections

The IT manager would like the service for the outgoing data stream to be tied to the destination of the Surveillance service site so that service can only be used for that one vendor.

To add the incoming service

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service**.
2. Fill out the fields with the following information

Name	WebCam_Connection-incoming
Comments	<Input into this field is optional>
Service Type	Firewall
Show in Service List	Check in check box
Category	Surveillance
Protocol Type	TCP/UDP/SCTP
IP/FQDN	<Leave blank>

	Destination Port		Source Port	
Protocol	Low	High	Low	High
TCP	8000	8000	1	65535
SCTP	16000	16000	1	65535

The source port range can be left blank as the default is 1 to 65635.

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service custom
   edit WebCam_Connection-incoming
      Set protocol TCP/UDP/SCTP
      Set tcp-portrange 8000
      Set sctp-portrange 16000
      Set visibility enable
   end
```

To add the outgoing service

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service**.
2. Fill out the fields with the following information

Name	WebCam_Connection-outgoing
Comments	<Input into this field is optional>
Service Type	Firewall
Color	<Changing this value is optional>
Show in Service List	Check in check box
Category	Surveillance
Protocol Type	TCP/UDP/SCTP
IP/FQDN	256.25.56.12

	Destination Port		Source Port	
Protocol	Low	High	Low	High
TCP	4000	4000	1	65535

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service custom
   edit WebCam_Connection-incoming
      Set protocol TCP/UDP/SCTP
      Set category Surveillance
      Set udp-portrange 4000
      Set iprange 256.25.56.12
      Set visibility enable
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services.** Check that the services have been added to the service list and that they are correct.
2. Enter the following CLI command:

```
config firewall service custom
   edit <the name of the service that you wish to verify>
      Show full-configuration
```

This should bring up all of the details of the service.

Example: ICMP service

The Security Officer would like to block the use of the traceroute utility through the network. The IT manager insists that ping and other ICMP utility must be allows for the task of diagnosing connectivity, so it is agreed that only traceroute functionality will be blocked.

The ICMP type for traceroute is 30. There is no codes with the type.

Web-based Manager Instructions

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service**.
2. Fill out the fields with the following information

Name	traceroute
Comments	<Input into this field is optional>
Service Type	Firewall
Show in Service List	Check in check box
Category	Uncategorized
Protocol Type	ICMP
Type	30
Code	<Leave blank>

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service custom
```

```
edit traceroute
   set protocol ICMP
   set icmptype 30
   set visibility enable
end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services.** Check that the services have been added to the services list and that they are correct.
2. Enter the following CLI command:

```
config firewall service custom
   edit <the name of the service that you wish to verify>
      show full-configuration
```

Example: ICMPv6 service

The IT Manager is doing some diagnostics and would like to temporarily block the successful replies of ICMP Node information Responses between 2 IPv6 networks.

The ICMP type for ICMP Node informations responses is 140. The codes for a successful response is 0.

Web-based Manager Instructions

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service**.
2. Fill out the fields with the following information

Name	diagnostic-test1
Comments	<Input into this field is optional>
Service Type	Firewall
Show in Service List	Check in check box
Category	Uncategorized
Protocol Type	ICMP6
Type	140
Code	0

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service custom
   edit diagnostic-test1
      set protocol ICMP6
      set icmptype 140
      set icmpcode 0
      set visibility enable
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services.** Check that the services have been added to the services list and that they are correct.
2. Enter the following CLI command:

```
config firewall service custom
   edit <the name of the service that you wish to verify>
      show full-configuration
```

Example: Service group

The company provide email services for a number of different companies. They have a standard list of services that they like to keep open to their customer's email servers, including webmail services. The company prides itself on getting a customer up and going the same day so they use standard templates for everything to make sure nothing is forgotten including the services that are available. The services include:

- IMAP
- IMAPS
- POP3
- POP3S
- SMTP
- SMTPS
- HTTP
- HTTPS
- Email_Admin - a custom service for administration of the servers

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service Group**.
2. Fill out the fields with the following information:

Group Name	Cust_Email_Serv_Template
Comments	(Optional)
Type	Firewall
Members	(click to add…choose from the drop down) • IMAP • IMAPS • POP3 • POP3S • SMTP • SMTPS • HTTP • HTTPS • Email_Admin

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service group
   edit Cust_Email_Serv_Template
```

```
    set member "IMAP" "IMAPS" "POP3" "POP3S" "SMTP" "SMTPS" "HTTP" "HTTPS" "Email_
        Admin"
    next
end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services.** Check that the service group has been added to the services list and that it is correct.
2. Enter the following CLI command:

```
config firewall service group
  edit <the name of the service that you wish to verify>
    show full-configuration
```

Example: Virtual IP address

The company has an web server on the internal network that needs to be accessed from the Internet.

- The internal IP address is 192.168.50.37
- The external IP address is 256.85.94.60 (for example use only. Not a valid IP address)
- The external IP address is assigned by ISP "A" on WAN1
- The port that needs to be mapped is 80

1. Go to **Policy & Objects > Objects> Virtual IPs** and select **Create New**.
2. Fill out the fields with the following information.

VIP Type	IPv4
Name	Web1-VIP
Comments	Virtual IP for the Forum Webserver
Interface	wan1
Type	(This field can only be changed in the CLI)
Source Address Filter	<disabled>
External IP Address/Range	256.85.94.60
Mapped IP Address/Range	192.168.50.37
Port Forwarding	<enabled>
Protocol	TCP
External Service Port	80
Map to Port	80

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall vip
  edit Web1-VIP
    set comment "Virtual IP for the Forum Webserver"
```

```
      set extintf wan1
      set extip 256.85.94.60
      set mappedip 192.168.50.37
      set portforward enable
      set protocol tcp
      set extport 80
      set mapped port 80
   end
end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects> Virtual IPs.** Check that the virtual IP address has been added to the list and that it is correct.
2. Enter the following CLI command:

```
config firewall vip
   edit <the name of the vip that you wish to verify>
      show full-configuration
```

VIP group

The company has only a single external IP address but multiple servers with different functions running on its internal LAN that need to be accessed from the Internet.

- The external IP address of the company on wan1 is 256.34.56.149 (for example use only. Not a valid IP address)
- The webserver is on the internal LAN on 192.168.100.86
- The webserver needs to answer on ports 80 443
- The administration of the FortiGate firewall connects on port 4443 instead of 443
- There is are also a separate email server, FTP server, and Terminal Server for specialised applications.
- 2 Virtual IPs have been created to map 256.34.56.149 to 192.168.100.86 on ports 80 and 443. The names are webserver_80 and webserver_443 respectively.

1. Go to **Policy & Objects > Objects> Virtual IPs**and select *Create New* > *Virtual IP Group.*
2. Fill out the fields with the following information.

Type	IPv4 VIP Group
Name	WebServer_Grp
Comments	(Optional)
Interface	wan1
Members	webserver_80 webserver_443

3. Enter the following CLI command:

```
config firewall vipgrp
   edit WebServer_Grp
      set member "webserver_80" "webserver_443"
      next
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Virtual IPs.** Check that the virtual IP address group has been added to the list and that it is correct.
2. Enter the following CLI command:

```
config firewall vipgrp
   edit <the name of the vip that you wish to verify>
      show full-configuration
```

Example: IP pool

Your company has an application server on the internal network that sends out regular data updates to an offsite service. In order to make the service site more secure, they only accept connections from predefined IP address. If the external IP address of the FortiGate firewall interface were used that would mean that the service would be accepting sessions from just about any user in the network so a separate IP address need so be assigned for the Network Address Translation.

- The external address that will be used is one that has been assigned to the company by the ISP on WAN2
- The address is 256.100.42.129 (for example use only. Not a valid IP address)

The ARP interface cannot be set in the Web-based Manager but as this is the only path that the traffic will be coming from the outside this should not be an issue. The setting has been included in the CLI instructions so that you will now how to set it in a situation where you want the ARP replies to be answered only on a specific interface.

1. Go to **Policy & Objects > Objects > IP Pools**.
2. Fill out the fields with the following information:

IP Pool Type	IPv4 Pool
Name	App_Server1
Comments	Addresses assignment for this server only.
Type	One-to-One
External IP Range	256.100.42.129
ARP Reply	<enabled>

3. Select **OK**.
4. Enter the following CLI command:

```
config firewall ippool
   edit App_Server1
      set comments ''Addresses assignment for this server only."
      set type one-to-one
      set arp-reply enable
      set arp-intf wan2
      set startip 256.100.42.129
      set endip 256.100.42.129
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > IP Pools**.
2. Check that the IP Pool has been added to the list of IP Pools and that the listed settings are correct.
3. Enter the following CLI command:

```
config firewall ippool
   edit <the name of the IP Pool you wish to verify>
      show full-configuration
```

Example: Central NAT table

The company has a server on the Development LAN that needs to communicate with a server at a remote site over the Internet. One of the restrictions on the communications between these systems is that the IP address and source port must be specific.

- The traffic going out on to the Internet must be NATed
- The traffic is coming from a server with the IP address 192.168.150.86
- An address called “app-server” has been created for the address 192.168.150.86 on the port1 interface
- The external interface must be 256.23.45.67
- An address called "app-server-ext" has been created for the address 256.23.45.67 on the wan1 interface
- The originating traffic from the server originates in the port range from 2000 to 3000
- The remote site requires that the source TCP port must be within the 12000 to 13000 range

The original address and Translated Address fields require values that are address names that are listed in the address section of Firewall Objects.

1. Go to **Policy & Objects > Policy > Central NAT > Create New** .
2. Fill out the fields with the following information:

Source Address	app-server
Translated Address	app-server-ext
Original Source Port	2000
Translated Port	12000-13000

3. Select **OK**.
4. Enter the following CLI command:

```
config firewall central-nat
   edit 0
      set orig-addr app-server
      set nat-ippool app-server-ext
      set orig-port 2000
      set nat-port 12000-13000
      next
   end
```

To verify that the table was added correctly:

1. Go to **Policy & Objects > Policy > Central NAT**.
2. Check that the table has been added to the list of Central NAT Tables and that the listed settings are correct.

3. Enter the following CLI command:

```
config firewall central-nat
   show full-configuration
```

4. Verify that the listing of tables includes the one that you have just configured, with the correct settings.

When configuring the Central NAT in the GUI you may notice that only those addresses which have been configured to be associated with **any** interface are displayed in the drop down menu for choosing a Source Address and yet the CLI will allow any address to be used, not just those associated with **any** interface. This is because by default the policies in the GUI use a function of cross referencing which addresses are allowed based on which interface is involved in the policy. When combined with the aspect of Central NAT that doesn't restrict to a specific interface. This means the only addresses will be allowed are those associated with the **any** interface. The CLI does not have this cross referencing function which is why the CLI seems less restrictive. However, more care must be taken when using the CLI to make sure that appropriate addresses are used.

Example: Firewall schedule - recurring

The Company wants to allow the use of Facebook by employees, but only during none business hours and the lunch break.

- The business hours are 9:00 p.m. to 6:00 p.m.
- The Lunch break is 12:00 p.m. to 1:00 p.m.
- The plan is to create a schedule to cover the morning business hours and the afternoon business hours and block access to the Facebook web site during that time.

1. Go to **Policy & Objects > Objects > Schedule**.
2. Select **Create New > Schedule**.
3. Fill out the fields with the following information:

Type	Recurring
Name	Morning_Business_Hours
Days	Monday, Tuesday, Wednesday, Thursday, Friday
Start Time	Hour = 9, Minute = 0
Stop Time	Hour = 12, Minute = 0

4. Select **OK**.
5. Enter the following CLI command:

```
config firewall schedule recurring
   edit Morning_Business_Hours
      set day monday tuesday wednesday thursday friday
      set start 09:00
      set end 12:00
   end
```

6. Create a second new schedule.

Type	Recurring
Name	Morning_Business_Hours
Days	Monday, Tuesday, Wednesday, Thursday, Friday
Start Time	Hour = 13, Minute = 0
Stop Time	Hour = 18, Minute = 0

7. Select **OK**.
8. Enter the following CLI command:

```
config firewall schedule recurring
   edit Afternoon_Business_Hours
      set day monday tuesday wednesday thursday friday
      set start 13:00
      set end 18:00
   end
```

To verify that the schedule was added correctly:

1. Go to **Policy & Objects > Objects > Schedule**.
2. Check that the schedule with the name you used has been added to the list of recurring schedules and that the listed settings are correct.
3. Enter the following CLI command:

```
config firewall schedule recurring
   edit <the name of the schedule you wish to verify>
      show full-configuration
```

Example: Firewall schedule - one-time

The company wants to change over their web site image to reference the new year. They have decided to take this opportunity to do some hardware upgrades as well. Their web site is business oriented so they have determined that over New Year's Eve there will be very limited traffic.

- They are going to need a maintenance window of 2 hours bracketing midnight on New Year's Eve.

1. Go to **Policy & Objects > Objects > Schedule**.
2. Select **Create New > Schedule**.
3. Fill out the fields with the following information:

Type	One-time
Name	NewYearsEve_Maintenance
Start Date	2014/12/31 <use the built in calendar>
End Date	2015/01/01 <use the built in calendar>
Start Time	Hour: 23, Minute: 0
Stop Time	Hour: 1Minute: 0

Pre-expiration event log	<disable>

4. Select **OK**.
5. Enter the following CLI command:

```
config firewall schedule onetime
   edit maintenance_window
      set start 23:00 2012/12/31
      set end 01:00 2013/01/01
      next
   end
```

To verify that the schedule was added correctly:

1. Go to **Policy & Objects > Objects > Schedule**.
2. Check that the schedule with the name you used has been added to the list of recurring schedules and that the listed settings are correct.
3. Enter the following CLI command:

```
config firewall schedule onetime
   edit <the name of the schedule you wish to verify>
      show full-configuration
   group you wish to verify>
      show full-configuration
```

Example: Schedule group

In order to make the administration of the policies easier a group needs to be created.

1. Go to **Policy & Objects > Objects > Schedule**.
2. Select **Create New > Schedule Group**.
3. Fill out the fields with the following information:

Name	Business_Hours
Members	Morning_Business_Hours Afternoon_Business_Hours

4. Select **OK**.
5. Enter the following CLI command:

```
config firewall service group
   edit Business_Hours
      set member Morning_Business_Hours Afternoon_Business _ours
   end
```

To verify that the schedule was added correctly:

1. Go to **Policy & Objects > Objects > Schedule**.
2. Check that the schedule group with the name you used has been added to the list of schedule groups.
3. Enter the following CLI command:

```
config firewall service group
   edit <the name of the schedule
```

Example: Proxy option

The company will be using a number of the Security Profiles features on various policies but wants to use as few profiles as possible to make administration simpler. The decision has been made to have two profiles, the default one and a single customized one that will be a combination of the settings required to cover the situations that will not be covered by the default profile.

The company profile will have the following parameters:

- There are no FTP servers running on the site so there is no need for FTP.
- The company has a non-standard IMAP implementation the uses port 1143.
- The Comfort Clients is to be used with a ratio of 1 byte for every 15 seconds.
- There is a lot of varied email traffic so there is to be no blocking of emails due to size beyond the settings on the mail servers.

1. Go to **Policy & Objects > Policy > Proxy Options**.
2. Create a new profile
3. Fill out the fields with the following information:

Name	example_standard
Comments	<optional>
Log Oversized Files	<disabled>

Protocol port mapping:

Enable	Protocol	Inspection Ports
enabled	HTTP	Specify and <leave on default setting.>
enabled	SMTP	Specify and <leave on default setting.>
enabled	POP3	Specify and <leave on default setting.>
enabled	IMAP	Specify and 1143
not enabled	FTP	
enabled	NNTP	Specify and <leave on default setting.>
enabled	MAPI	<leave on default setting.>
enabled	DNS	<leave on default setting.>

Common options

Comfort Clients	enabled
Interval (Seconds)	15
Amount(bytes)	1
Block Oversized File/Email	not enabled
Threshold(MB)	not enabled

Web options

Enabled Chunked Bypass	not enabled
Add Fortinet Bar	not enabled
Communication Port	<Unseen because Add Fortinet Bar is not enabled>

Email Options

Allow Fragmented Messages	<not enabled>
Append Signature (SMTP)	<not enabled>
Email Signature Text	<Unseen because Append Signature is not enabled>

4. Select **OK**.
5. Enter the following CLI command:

```
config firewall profile-protocol-options
   edit example_standard
      config http
         set options clientcomfort no-content-summary
         set comfort-interval 15
         next
      config ftp
         set status disable
         set options clientcomfort no-content-summary splice
         set comfort-interval 15
         next
      config imap
         set ports "1143"
         set options fragmail no-content-summary
         next
      config mapi
         set options fragmail no-content-summary
         next
      config pop3
         set options fragmail no-content-summary
```

```
    next
  config smtp
    set options fragmail no-content-summary splice
    next
  config nntp
    set options no-content-summary splice
    next
  config ssh
    set inspect-all enable
    set log x11-filter ssh-shell exec port-forward
    next
  end
```

Oversized files

A couple of variations on the example could have to do with the processing of oversized files at a level other than the default setting. The ways that it can be approached are:

Set a non default threshold size and block the files

Set a non default threshold size and not scan the files over the threshold but allow them to pass through the FortiGate firewall.

In the following instructions:

- We will just use 2 MB as the new threshold.
- In the CLI instructions we will limit the configuration to just the HTTP settings for the purposes of brevity and simplicity.

Option 1

Option 1 can be done in the GUI.

1. Go to **Policy & Objects > Policy > Proxy Options**.
2. Edit the profile that you wan the change in.
3. Fill out the fields with the following information:

Common Options

Comfort Clients	enabled
Interval (Seconds)	15
Amount(bytes)	1
Block Oversized File/Email	enabled
Threshold(MB)	2

4. Select **OK**.
5. Enter the following CLI command:

```
config firewall profile-protocol-options
  edit example_standard
    config http
```

```
      set options clientcomfort no-content-summary oversize
      set oversize-limit 2
      set comfort-interval 15
      next
   end
```

Option 2

Option 2 can only be done in the CLI. Enter the following CLI command:

```
config firewall profile-protocol-options
   edit example_standard
      config http
         set options clientcomfort no-content-summary
         set oversize-limit 2
         set comfort-interval 15
         next
      end
```

Example: DoS policy

The company wishes to protect against Denial of Service attach. They have chosen some where they wish to block the attacks of the incidence goes above a certain threshold and for some others they are just trying to get a baseline of activity for those types of attacks so they are letting the traffic pass through without action.

- The interface to the Internet is on WAN1
- There is no requirement to specify which addresses are being protected or protected from.
- The protection is to extend to all services.
- The TCP attacks are to be blocked
- The UDP, ICMP, and IP attacks are to be recorded but not blocked.
- The tcp_syn_flood attach's threshold is to be changed from the default to 1000

1. Go to **Policy & Objects > Policy > DoS**.
2. Create a new policy
3. Fill out the fields with the following information:

Incoming Interface	wan1
Source Address	all
Destination Addresses	all
Service	ALL

Anomalies

Name	Status	Logging	Action	Threshold
tcp_syn_flood	enabled	enabled	Block	1000
tcp_port_scan	enabled	enabled	Block	<default value>
tcp_src_session	enabled	enabled	Block	<default value>
tcp_dst_session	enabled	enabled	Block	<default value>
udp_flood	enabled	enabled	Pass	<default value>
udp_scan	enabled	enabled	Pass	<default value>
udp_src_session	enabled	enabled	Pass	<default value>
udp_dst_session	enabled	enabled	Pass	<default value>
icmp_flood	enabled	enabled	Pass	<default value>
icmp_sweep	enabled	enabled	Pass	<default value>
icmp_src_session	enabled	enabled	Pass	<default value>
icmp_dst_session	enabled	enabled	Pass	<default value>
ip_src_session	enabled	enabled	Pass	<default value>
ip_dst_session	enabled	enabled	Pass	<default value>
sctp_flood	not enabled	not enabled	Pass	<default value>
sctp_scan	not enabled	not enabled	Pass	<default value>
sctp_src_session	not enabled	not enabled	Pass	<default value>
sctp_dst_session	not enabled	not enabled	Pass	<default value>

4. Toggle the button next to **Enable this policy** to **ON**.
5. Select **OK**.
6. Enter the following CLI command:

```
config firewall DoS-policy
   edit 0
      set status enable
      set interface ''
      config anomaly
         edit "tcp_syn_flood"
            set status enable
            set log enable
            set action block
```

```
      set threshold 1000
      next
   edit "tcp_port_scan"
      set status enable
      set log enable
      set action block
      next
   edit "tcp_src_session"
      set status enable
      set log enable
      set action block
      next
   edit "tcp_dst_session"
      set status enable
      set log enable
      set action block
   next
      edit "udp_flood"
      set status enable
      set log enable
   next
      edit "udp_scan"
      set status disable
      set status enable
      set log enable
      next
   edit "udp_src_session"
      set status enable
      set log enable
      next
   edit "udp_dst_session"
      set status enable
      set log enable
      next
   edit "icmp_flood"
      set status enable
      set log enable
      next
   edit "icmp_sweep"
      set status enable
      set log enable
      next
   edit "icmp_src_session"
      set status enable
      set log enable
      next
   edit "icmp_dst_session"
      set status enable
      set log enable
      next
   edit "ip_src_session"
      set status enable
      set log enable
      next
   edit "ip_dst_session"
      set status enable
      set log enable
```

```
        next
      end
    next
  end
```

Multicast forwarding

Multicasting (also called IP multicasting) consists of using a single multicast source to send data to many receivers. Multicasting can be used to send data to many receivers simultaneously while conserving bandwidth and reducing network traffic. Multicasting can be used for one-way delivery of media streams to multiple receivers and for one-way data transmission for news feeds, financial information, and so on.

Also RIPv2 uses multicasting to share routing table information, OSPF uses multicasting to send hello packets and routing updates, Enhanced Interior Gateway Routing Protocol (EIGRP) uses multicasting to send routing information to all EIGRP routers on a network segment and the Bonjour network service uses multicasting for DNS.

A FortiGate unit can operate as a Protocol Independent Multicast (PIM) version 2 router. FortiGate units support PIM sparse mode (RFC 4601) and PIM dense mode (RFC 3973) and can service multicast servers or receivers on the network segment to which a FortiGate unit interface is connected. Multicast routing is not supported in transparent mode (TP mode).

To support PIM communications, the sending/receiving applications and all connecting PIM routers in between must be enabled with PIM version 2. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations. To enable source-to-destination packet delivery, either sparse mode or dense mode must be enabled on the PIM-router interfaces. Sparse mode routers cannot send multicast messages to dense mode routers. In addition, if a FortiGate unit is located between a source and a PIM router, two PIM routers, or is connected directly to a receiver, you must create a security policy manually to pass encapsulated (multicast) packets or decapsulated data (IP traffic) between the source and destination.

A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one Boot Strap Router (BSR), and if sparse mode is enabled, a number of Rendezvous Points (RPs) and Designated Routers (DRs). When PIM is enabled on a FortiGate unit, the FortiGate unit can perform any of these functions at any time as configured.

Sparse mode

Initially, all candidate BSRs in a PIM domain exchange bootstrap messages to select one BSR to which each RP sends the multicast address or addresses of the multicast group(s) that it can service. The selected BSR chooses one RP per multicast group and makes this information available to all of the PIM routers in the domain through bootstrap messages. PIM routers use the information to build packet distribution trees, which map each multicast group to a specific RP. Packet distribution trees may also contain information about the sources and receivers associated with particular multicast groups.

When a FortiGate unit interface is configured as a multicast interface, sparse mode is enabled on it by default to ensure that distribution trees are not built unless at least one downstream receiver requests multicast traffic from a specific source. If the sources of multicast traffic and their receivers are close to each other and the PIM domain contains a dense population of active receivers, you may choose to enable dense mode throughout the PIM domain instead.

An RP represents the root of a non-source-specific distribution tree to a multicast group. By joining and pruning the information contained in distribution trees, a single stream of multicast packets (for example, a video feed) originating from the source can be forwarded to a certain RP to reach a multicast destination.

Each PIM router maintains a Multicast Routing Information Base (MRIB) that determines to which neighboring PIM router join and prune messages are sent. An MRIB contains reverse-path information that reveals the path of a multicast packet from its source to the PIM router that maintains the MRIB.

To send multicast traffic, a server application sends IP traffic to a multicast group address. The locally elected DR registers the sender with the RP that is associated with the target multicast group. The RP uses its MRIB to forward a single stream of IP packets from the source to the members of the multicast group. The IP packets are replicated only when necessary to distribute the data to branches of the RP's distribution tree.

To receive multicast traffic, a client application can use Internet Group Management Protocol (IGMP) version 1 (RFC 1112), 2 (RFC 2236), or 3 (RFC 3376) control messages to request the traffic for a particular multicast group. The locally elected DR receives the request and adds the host to the multicast group that is associated with the connected network segment by sending a join message towards the RP for the group. Afterward, the DR queries the hosts on the connected network segment continually to determine whether the hosts are active. When the DR no longer receives confirmation that at least one member of the multicast group is still active, the DR sends a prune message towards the RP for the group.

FortiOS supports PIM sparse mode multicast routing for IPv6 multicast (multicast6) traffic and is compliant with RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM). You can use the following command to configure IPv6 PIM sparse multicast routing.

```
config router multicast6
   set multicast-routing {enable | disable}
      config interface
         edit <interface-name>
            set hello-interval <1-65535 seconds>
            set hello-holdtime <1-65535 seconds>
         end
      config pim-sm-global
         config rp-address
            edit <index>
               set ipv6-address <ipv6-address>
            end
```

The following diagnose commands for IPv6 PIM sparse mode are also available:

```
diagnose ipv6 multicast status
diagnose ipv6 multicast vif
diagnose ipv6 multicast mroute
```

Dense mode

The packet organization used in sparse mode is also used in dense mode. When a multicast source begins to send IP traffic and dense mode is enabled, the closest PIM router registers the IP traffic from the multicast source (S) and forwards multicast packets to the multicast group address (G). All PIM routers initially broadcast the multicast packets throughout the PIM domain to ensure that all receivers that have requested traffic for multicast group address G can access the information if needed.

To forward multicast packets to specific destinations afterward, the PIM routers build distribution trees based on the information in multicast packets. Upstream PIM routers depend on prune/graft messages from downstream PIM routers to determine if receivers are actually present on directly connected network segments. The PIM

routers exchange state refresh messages to update their distribution trees. FortiGate units store this state information in a Tree Information Base (TIB), which is used to build a multicast forwarding table. The information in the multicast forwarding table determines whether packets are forwarded downstream. The forwarding table is updated whenever the TIB is modified.

PIM routers receive data streams every few minutes and update their forwarding tables using the source (S) and multicast group (G) information in the data stream. Superfluous multicast traffic is stopped by PIM routers that do not have downstream receivers—PIM routers that do not manage multicast groups send prune messages to the upstream PIM routers. When a receiver requests traffic for multicast address G, the closest PIM router sends a graft message upstream to begin receiving multicast packets.

FortiGate units operating in NAT mode can also be configured as multicast routers. You can configure a FortiGate unit to be a Protocol Independent Multicast (PIM) router operating in Sparse Mode (SM) or Dense Mode (DM).

Multicast IP addresses

Multicast uses the Class D address space. The 224.0.0.0 to 239.255.255.255 IP address range is reserved for multicast groups. The multicast address range applies to multicast groups, not to the originators of multicast packets. The following table lists the reserved multicast address ranges and describes what they are reserved for:

Reserved Multicast address ranges

Reserved Address Range	Use	Notes
224.0.0.0 to 224.0.0.255	Used for network protocols on local networks. For more information, see RFC 1700.	In this range, packets are not forwarded by the router but remain on the local network. They have a Time to Live (TTL) of 1. These addresses are used for communicating routing information.
224.0.1.0 to 238.255.255.255	Global addresses used for multicasting data between organizations and across the Internet. For more information, see RFC 1700.	Some of these addresses are reserved, for example, 224.0.1.1 is used for Network Time Protocol (NTP).
239.0.0.0 to 239.255.255.255	Limited scope addresses used for local groups and organizations. For more information, see RFC 2365.	Routers are configured with filters to prevent multicasts to these addresses from leaving the local system.

Creating multicast security policies requires multicast firewall addresses. You can add multicast firewall addresses by going to **Firewall Objects > Address > Addresses** and selecting **Create New > Multicast Address**. The factory default configuration includes multicast addresses for Bonjour (224.0.0.251-224.0.0.251, EIGRP (224.0.0.10-224.0.0.100), OSPF (224.0.0.5-224.0.0.60), all_hosts (224.0.0.1-224.0.0.1), and all_routers (224.0.0.2-224.0.0.2).

PIM Support

A FortiGate unit can be configured to support PIM by going to **Router > Dynamic > Multicast** and enabling multicast routing. You can also enable multicast routing using the `config router multicast` CLI

command. When PIM is enabled, the FortiGate unit allocates memory to manage mapping information. The FortiGate unit communicates with neighboring PIM routers to acquire mapping information and if required, processes the multicast traffic associated with specific multicast groups.

The end-user multicast client-server applications must be installed and configured to initiate Internet connections and handle broadband content such as audio/video information.

Client applications send multicast data by registering IP traffic with a PIM-enabled router. An end-user could type in a class D multicast group address, an alias for the multicast group address, or a call-conference number to initiate the session.

Rather than sending multiple copies of generated IP traffic to more than one specific IP destination address, PIM-enabled routers encapsulate the data and use the one multicast group address to forward multicast packets to multiple destinations. Because one destination address is used, a single stream of data can be sent. Client applications receive multicast data by requesting that the traffic destined for a certain multicast group address be delivered to them — end-users may use phone books, a menu of ongoing or future sessions, or some other method through a user interface to select the address of interest.

A class D address in the 224.0.0.0 to 239.255.255.255 range may be used as a multicast group address, subject to the rules assigned by the Internet Assigned Numbers Authority (IANA). All class D addresses must be assigned in advance. Because there is no way to determine in advance if a certain multicast group address is in use, collisions may occur (to resolve this problem, end-users may switch to a different multicast address).

To configure a PIM domain

1. If you will be using sparse mode, determine appropriate paths for multicast packets.
2. Make a note of the interfaces that will be PIM-enabled. These interfaces may run a unicast routing protocol.
3. If you will be using sparse mode and want multicast packets to be handled by specific (static) RPs, record the IP addresses of the PIM-enabled interfaces on those RPs.
4. Enable PIM version 2 on all participating routers between the source and receivers. On FortiGate units, use the `config router multicast` command to set global operating parameters.
5. Configure the PIM routers that have good connections throughout the PIM domain to be candidate BSRs.
6. If sparse mode is enabled, configure one or more of the PIM routers to be candidate RPs.
7. If required, adjust the default settings of PIM-enabled interface(s).

Multicast forwarding and FortiGate units

In both transparent mode and NAT mode you can configure FortiGate units to forward multicast traffic.

For a FortiGate unit to forward multicast traffic you must add FortiGate multicast security policies. Basic multicast security policies accept any multicast packets at one FortiGate interface and forward the packets out another FortiGate interface. You can also use multicast security policies to be selective about the multicast traffic that is accepted based on source and destination address, and to perform NAT on multicast packets.

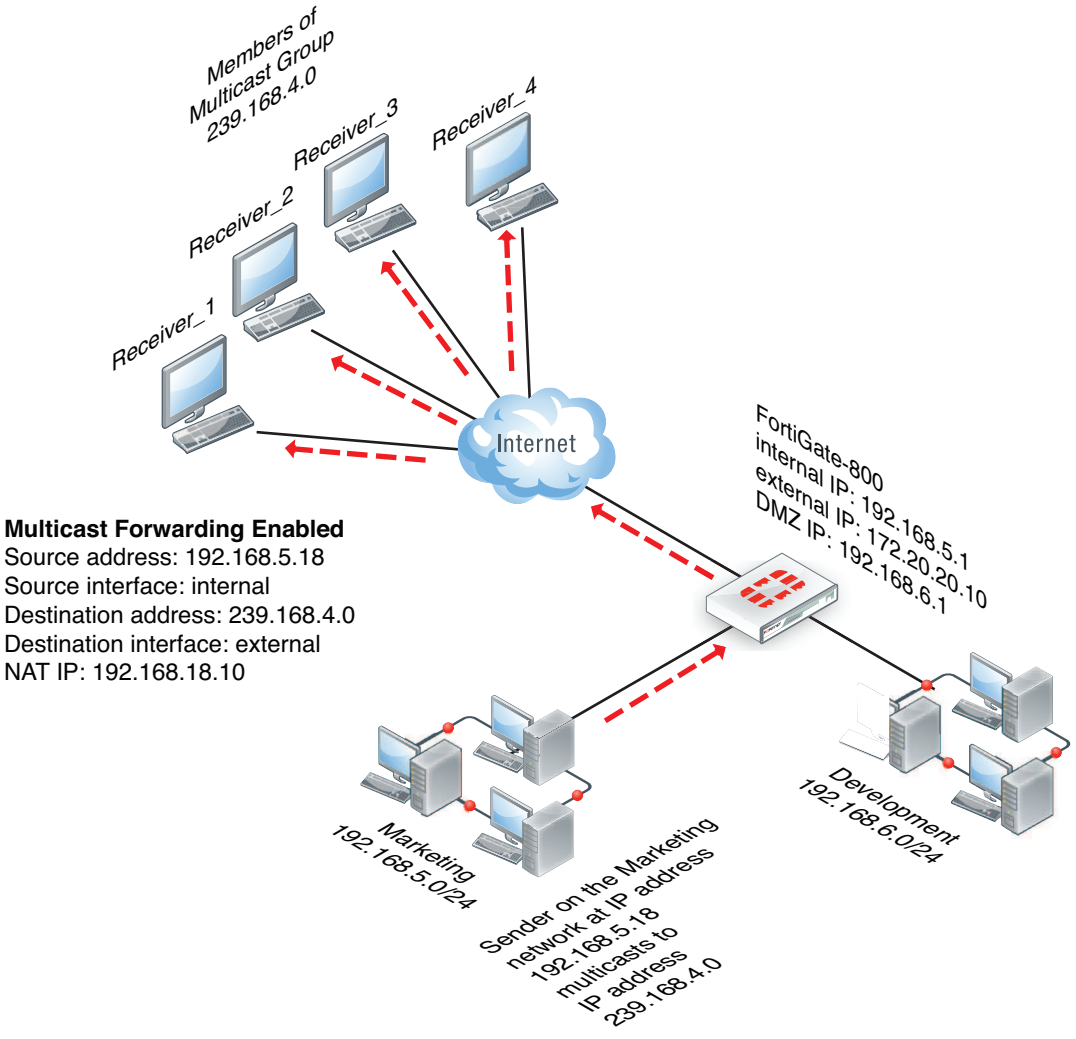
In the example shown below, a multicast source on the Marketing network with IP address 192.168.5.18 sends multicast packets to the members of network 239.168.4.0. At the FortiGate unit, the source IP address for multicast packets originating from workstation 192.168.5.18 is translated to 192.168.18.10. In this example, the FortiGate unit is not acting as a multicast router.

Multicast forwarding and RIPv2

RIPv2 uses multicast to share routing table information. If your FortiGate unit is installed on a network that includes RIPv2 routers, you must configure the FortiGate unit to forward multicast packets so that RIPv2 devices can share routing data through the FortiGate unit. No special FortiGate configuration is required to share RIPv2 data, you can simply use the information in the following sections to configure the FortiGate unit to forward multicast packets.

RIPv1 uses broadcasting to share routing table information. To allow RIPv1 packets through a FortiGate unit you can add standard security policies. Security policies to accept RIPv1 packets can use the ANY predefined firewall service or the RIP pre-defined firewall service.

Example multicast network including a FortiGate unit that forwards multicast packets



Configuring FortiGate multicast forwarding

You configure FortiGate multicast forwarding from the Command Line Interface (CLI). Two steps are required:

- Adding multicast security policies
- Enabling multicast forwarding
  This second step is only required if your FortiGate unit is operating in NAT mode. If your FortiGate unit is operating in transparent mode, adding a multicast policy enables multicast forwarding.

There is sometimes a confusion between the terms “forwarding” and “routing”. These two functions should not be taking place at the same time.

It is mentioned that multicast-forward should be enabled when the FortiGate unit is in NAT mode and that this will forward any multicast packet to all interfaces. However, this parameter should **NOT** be enabled when the FortiGate unit operates as a multicast router (i.e. with a routing protocol enabled. It should only be enabled when there is no routing protocols activated.

Adding multicast security policies

You need to add security policies to allow packets to pass from one interface to another. Multicast packets require multicast security policies. You add multicast security policies from the CLI using the `config firewall multicast-policy` command. As with unicast security policies, you specify the source and destination interfaces and optionally the allowed address ranges for the source and destination addresses of the packets.

You can also use multicast security policies to configure source NAT and destination NAT for multicast packets.

Keep the following in mind when configuring multicast security policies:

- The matched forwarded (outgoing) IP multicast source IP address is changed to the configured IP address.
- Source and Destination interfaces are optional. If left blank, then the multicast will be forwarded to ALL interfaces.
- Source and Destination addresses are optional. If left un set, then it will mean ALL addresses.
- The `nat` keyword is optional. Use it when source address translation is needed.

Enabling multicast forwarding

Multicast forwarding is enabled by default. In NAT mode you must use the `multicast-forward` keyword of the `system settings` CLI command to enable or disable multicast forwarding. When `multicast-forward` is enabled, the FortiGate unit forwards any multicast IP packets in which the TTL is 2 or higher to all interfaces and VLAN interfaces except the receiving interface. The TTL in the IP header will be reduced by 1. Even though the multicast packets are forwarded to all interfaces, you must add security policies to actually allow multicast packets through the FortiGate. In our example, the security policy allows multicast packets received by the internal interface to exit to the external interface.

Enabling multicast forwarding is only required if your FortiGate unit is operating in NAT mode. If your FortiGate unit is operating in transparent mode, adding a multicast policy enables multicast forwarding.

Enter the following CLI command to enable multicast forwarding:

```
config system settings
   set multicast-forward enable
end
```

If multicast forwarding is disabled and the FortiGate unit drops packets that have multicast source or destination addresses.

You can also use the `multicast-ttl-notchange` keyword of the `system settings` command so that the FortiGate unit does not increase the TTL value for forwarded multicast packets. You should use this option only if packets are expiring before reaching the multicast router.

```
config system settings
   set multicast-ttl-notchange enable
end
```

In transparent mode, the FortiGate unit does not forward frames with multicast destination addresses. Multicast traffic such as the one used by routing protocols or streaming media may need to traverse the FortiGate unit, and should not be interfere with the communication. To avoid any issues during transmission, you can set up multicast security policies. These types of security policies can only be enabled using the CLI.

The CLI parameter multicast-skip-policy must be disabled when using multicast security policies. To disable enter the command

```
config system settings
     set multicast-skip-policy disable
end
```

In this simple example, no check is performed on the source or destination interfaces. A multicast packet received on an interface is flooded unconditionally to all interfaces on the forwarding domain, except the incoming interface.

To enable the multicast policy

```
config firewall multicast-policy
   edit 1
      set action accept
   end
```

In this example, the multicast policy only applies to the source port of WAN1 and the destination port of Internal.

To enable the restrictive multicast policy

```
config firewall multicast-policy
   edit 1
      set srcintf wan1
      set dstinf internal
      set action accept
   end
```

In this example, packets are allowed to flow from WAN1 to Internal, and sourced by the address 172.20.120.129, which is represented by the address object "example_addr-1".

To enable the restrictive multicast policy

```
config firewall multicast-policy
   edit 1
      set srcintf wan1
      set srcaddr example_addr-1
      set dstinf internal
      set action accept
   end
```

This example shows how to configure the multicast security policy required for the configuration shown. This policy accepts multicast packets that are sent from a PC with IP address 192.168.5.18 to destination address

range 239.168.4.0. The policy allows the multicast packets to enter the internal interface and then exit the external interface. When the packets leave the external interface their source address is translated to 192.168.18.10

```
config firewall multicast-policy
   edit 5
      set srcaddr 192.168.5.18 255.255.255.255
      set srcintf internal
      set destaddr 239.168.4.0 255.255.255.0
      set dstintf external
      set nat 192.168.18.10
   end
```

This example shows how to configure a multicast security policy so that the FortiGate unit forwards multicast packets from a multicast Server with an IP 10.10.10.10 is broadcasting to address 225.1.1.1. This Server is on the network connected to the FortiGate DMZ interface.

```
config firewall multicast-policy
   edit 1
      set srcintf DMZ
      set srcaddr 10.10.10.10 255.255.255.255
      set dstintf Internal
      set dstaddr 225.1.1.1 255.255.255.255
      set action accept
   edit 2
      set action deny
   end
```

Multicast routing examples

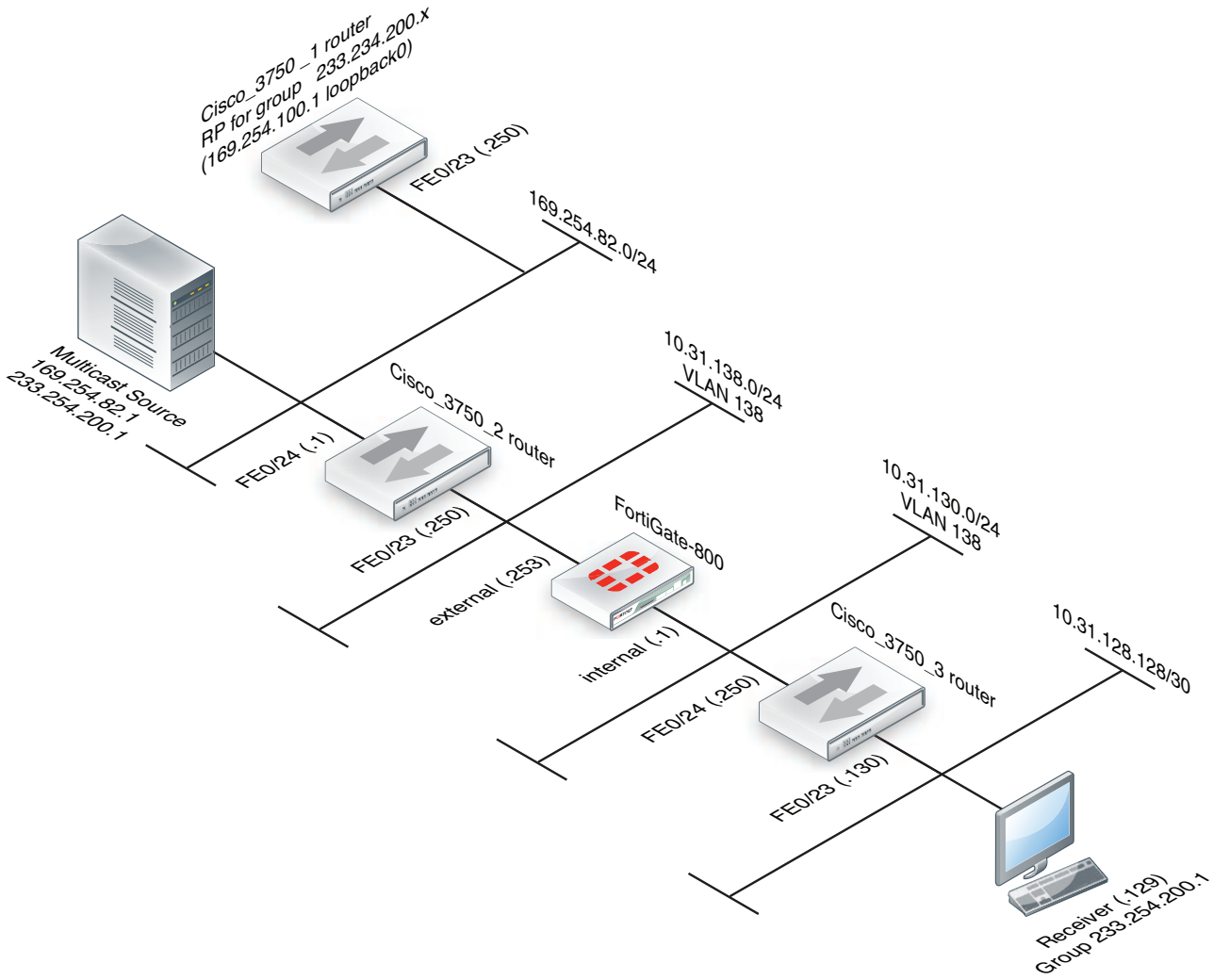
This section contains the following multicast routing configuration examples and information:

- Example FortiGate PIM-SM configuration using a static RP
- FortiGate PIM-SM debugging examples
- Example multicast destination NAT (DNAT) configuration
- Example PIM configuration that uses BSR to find the RP

Example FortiGate PIM-SM configuration using a static RP

The example Protocol Independent Multicast Sparse Mode (PIM-SM) configuration shown below has been tested for multicast interoperability using PIM-SM between Cisco 3750 switches running 12.2 and a FortiGate-800 running FortiOS v3.0 MR5 patch 1. In this configuration, the receiver receives the multicast stream when it joins the group 233.254.200.1.

Example FortiGate PIM-SM topology



The configuration uses a statically configured rendezvous point (RP) which resides on the Cisco_3750_1. Using a bootstrap router (BSR) was not tested in this example. See “Example PIM configuration that uses BSR to find the RP” for an example that uses a BSR.

Configuration steps

The following procedures show how to configure the multicast configuration settings for the devices in the example configuration.

- Cisco_3750_1 router configuration
- Cisco_3750_2 router configuration
- To configure the FortiGate-800 unit
- Cisco_3750_3 router configuration

Cisco_3750_1 router configuration

```
version 12.2
```

```
!
hostname Cisco-3750-1
!
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip multicast-routing distributed
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface Loopback0
   ip address 169.254.100.1 255.255.255.255
!
interface FastEthernet1/0/23
   switchport access vlan 182
   switchport mode access
!
interface FastEthernet1/0/24
   switchport access vlan 172
   switchport mode access
!
interface Vlan172
   ip address 10.31.138.1 255.255.255.0
   ip pim sparse-mode
   ip igmp query-interval 125
   ip mroute-cache distributed
!
interface Vlan182
   ip address 169.254.82.250 255.255.255.0
   ip pim sparse-mode
   ip mroute-cache distributed
!
ip classless
ip route 0.0.0.0 0.0.0.0 169.254.82.1
ip http server
ip pim rp-address 169.254.100.1 Source-RP
!
ip access-list standard Source-RP
   permit 233.254.200.0 0.0.0.255
```

Cisco_3750_2 router configuration

```
version 12.2
!
hostname Cisco-3750-2
!
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip multicast-routing distributed
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
```

```
spanning-tree extend system-id
!
interface FastEthernet1/0/23
   switchport access vlan 138
   switchport mode access
!
interface FastEthernet1/0/24
   switchport access vlan 182
   witchport mode access
!
interface Vlan138
   ip address 10.31.138.250 255.255.255.0
   ip pim sparse-mode
   ip mroute-cache distributed
!
interface Vlan182
   ip address 169.254.82.1 255.255.255.0
   ip pim sparse-mode
   ip mroute-cache distributed
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.138.253
ip route 169.254.100.1 255.255.255.255 169.254.82.250
ip http server
ip pim rp-address 169.254.100.1 Source-RP
!
!
ip access-list standard Source-RP
permit 233.254.200.0 0.0.0.255
```

To configure the FortiGate-800 unit

1. Configure the internal and external interfaces.

- **Internal**

  Go to **System > Network > Interfaces**.

  Select the internal interface.

  Verify the following settings:

Type:	Physical Interface
Addressing mode:	Manual
IP/Network Mask:	10.31.138.253 255.255.255.0
Administrative Access:	PING

  Select **OK**.

- **External**

  Go to **System > Network > Interfaces**.

Select the external interface.

Verify the following settings:

Type:	Physical Interface
Addressing mode:	Manual
IP/Network Mask:	10.31.130.253 255.255.255.0
Administrative Access:	HTTPS and PING

Select **OK**.

2. Add a firewall addresses.

Go to **Policy & Objects> Objects > Addresses.**

- RP

Select **Create New**.

Use the following settings:

Category:	Address
Name:	RP
Type:	Subnet
Subnet/IP Range:	169.254.100.1/32
Interface:	Any
Visibility:	<enabled>

Select **OK**.

- Multicast source subnet

Select **Create New**.

Use the following settings:

Category:	Address
Name:	multicast_source_subnet
Type:	Subnet
Subnet/IP Range:	169.254.82.0/24
Interface:	Any
Visibility:	<enabled>

Select **OK**.

3. Add destination multicast address

   Go to **Policy & Objects> Objects > Addresses.**

   Select **Create New**.

   Use the following settings:

Category:	Multicast Address
Name:	Multicast_stream
Type:	Broadcast Subnet
Broadcast Subnet:	233.254.200.0/24
Interface:	Any
Visibility:	<enabled>

   Select **OK**.

4. Add standard security policies to allow traffic to reach the RP.

   Go to **Policy & Objects > Policy > IPv4**.

   - 1st policy

   Select **Create New**

   Use the following settings:

Incoming Interface:	internal
Source Address:	all
Outgoing Interface:	external
Destination Address:	RP
Schedule:	always
Service:	ALL
Action:	ACCEPT

   Select **OK**.

   - 2nd policy

   Select **Create New**

   Use the following settings:

Incoming Interface:	external

Source Address:	RP
Outgoing Interface:	internal
Destination Address:	all
Schedule:	always
Service:	ALL
Action:	ACCEPT

Select **OK**.

5. Add the multicast security policy.

   Go to **Policy & Objects > Policy > Multicast**.

   Select **Create New**.

   Use the following settings:

Incoming Interface:	external
Source Address:	multicast_source_subnet
Outgoing Interface:	internal
Destination Address:	multicast_stream
Protocol:	Any
Action:	ACCEPT

   Select **OK**.

6. Add an access list. (CLI only)

```
config router access-list
   edit Source-RP
      config rule
         edit 1
            set prefix 233.254.200.0 255.255.255.0
            set exact-match disable
         next
      end
```

7. Add some static routes.

   Go to **Router > Static > Static Routes**.

   - Route 1

   Select **Create New**.

   Use the following settings:

Destination IP/Mask:	0.0.0.0/0.0.0.0
Device:	internal
Gateway:	10.31.130.250
Distance:	<default>
Priority:	<default>

Select **OK**.

- Route 2

Select **Create New**.

Use the following settings:

Destination IP/Mask:	169.254.0.0/16
Device:	external
Gateway:	10.31.138.250
Distance:	<default>
Priority:	<default>

Select **OK**.

8. Configure multicast routing.

   Go to **Router > Dynamic > Multicast**.

   Add the following Static Rendezvous Point(s):
   - 169.254.100.1

   - Route 1

   Select **Create New**.

   Use the following settings:

Interface:	internal
PIM Mode:	Sparse Mode
DR Priority:	<not needed in this scenario>
RP Candidate:	<not needed in this scenario>
RP Candidate Priority:	<not needed in this scenario>

   Select **OK.**

   - Route 2

Select **Create New**.

Use the following settings:

Interface:	external
PIM Mode:	Sparse Mode
DR Priority:	
RP Candidate:	
RP Candidate Priority:	

Select **OK.**

Cisco_3750_3 router configuration

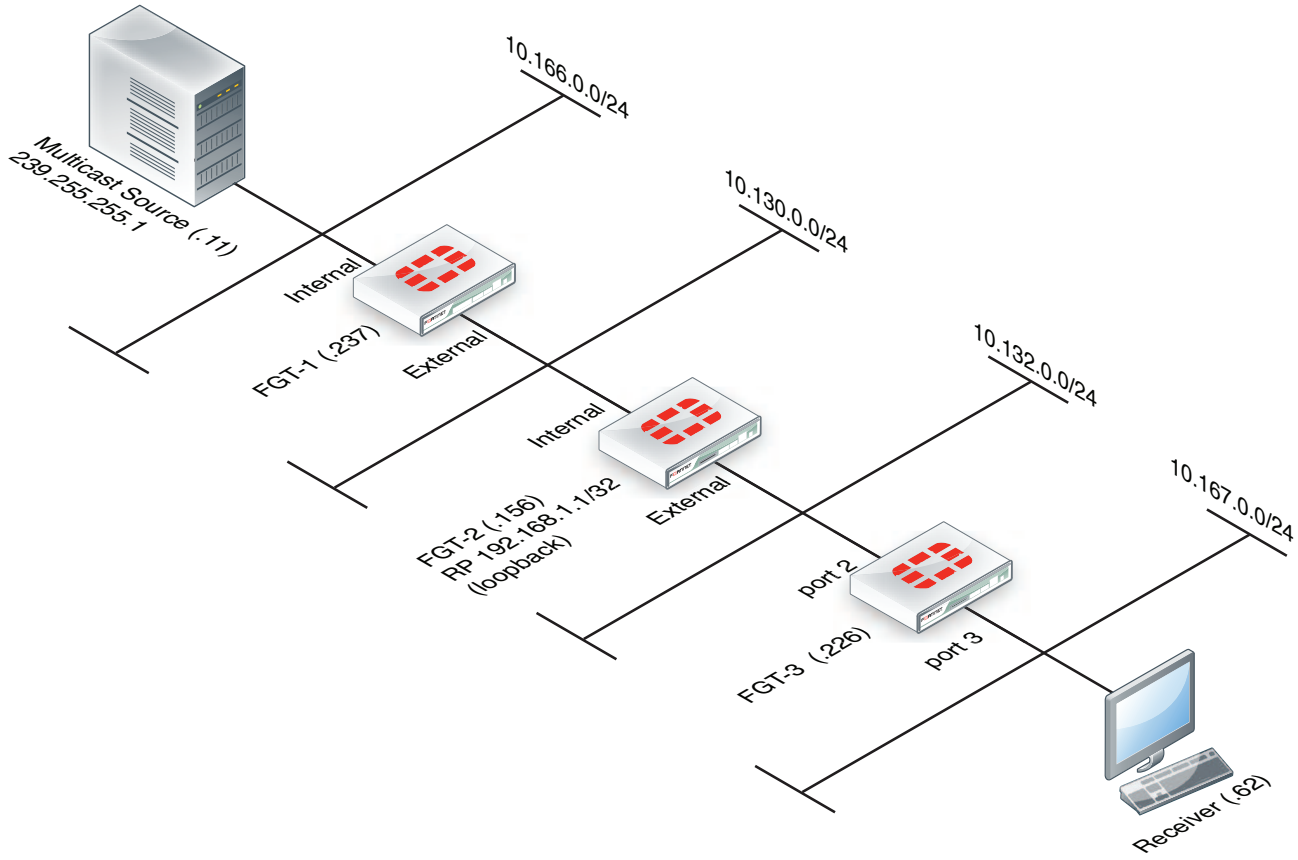
```
version 12.2
!
hostname Cisco-3750-3
!
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip multicast-routing distributed
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet1/0/23
   switchport access vlan 128
   switchport mode access
!
interface FastEthernet1/0/24
   switchport access vlan 130
   switchport mode access
!
interface Vlan128
   ip address 10.31.128.130 255.255.255.252
   ip pim sparse-mode
   ip mroute-cache distributed
!
interface Vlan130
   ip address 10.31.130.250 255.255.255.0
   ip pim sparse-mode
   ip mroute-cache distributed
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.130.1
ip http server
ip pim rp-address 169.254.100.1 Source-RP
!
!
ip access-list standard Source-RP
```

```
permit 233.254.200.0 0.0.0.255
```

FortiGate PIM-SM debugging examples

Using the example topology shown below, you can trace the multicast streams and states within the three FortiGate units (FGT-1, FGT-2, and FGT-3) using the debug commands described in this section. The command output in this section is taken from FortiGate unit when the multicast stream is flowing correctly from source to receiver.

PIM-SM debugging topology



Checking that the receiver has joined the required group

From the last hop router, FGT-3, you can use the following command to check that the receiver has correctly joined the required group.

```
FGT-3 # get router info multicast igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
239.255.255.1 port3 00:31:15 00:04:02 10.167.0.62
```

Only 1 receiver is displayed for a particular group, this is the device that responded to the IGMP query request from the FGT-3. If a receiver is active the expire time should drop to approximately 2 minutes before being refreshed.

Checking the PIM-SM neighbors

Next the PIM-SM neighbors should be checked. A PIM router becomes a neighbor when the PIM router receives a PIM hello. Use the following command to display the PIM-SM neighbors of FGT-3.

```
FGT-3 # get router info multicast pim sparse-mode neighbour
Neighbor Interface Uptime/Expires Ver DR
Address Priority/Mode
10.132.0.156 port2 01:57:12/00:01:33 v2 1 /
```

Checking that the PIM router can reach the RP

The rendezvous point (RP) must be reachable for the PIM router (FGT-3) to be able to send the `*,G` join to request the stream. This can be checked for FGT-3 using the following command:

```
FGT-3 # get router info multicast pim sparse-mode rp-mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
RP: 192.168.1.1
Uptime: 07:23:00
```

Viewing the multicast routing table (FGT-3)

The FGT-3 unicast routing table can be used to determine the path taken to reach the RP at 192.168.1.1. You can then check the stream state entries using the following commands:

```
FGT-3 # get router info multicast pim sparse-mode table
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
```

(*,*,RP) Entries	This state may be reached by general joins for all groups served by a specified RP.
(*,G) Entries	State that maintains the RP tree for a given group.
(S,G) Entries	State that maintains a source-specific tree for source `S` and group `G`.
(S,G,rpt) Entries	State that maintains source-specific information about source s on the RP tree for `G`. For example, if a source is being received on the source-specific tree, it will normally have been pruned off the RP tree.
FCR	The FCR state entries are for tracking the sources in the <*, G> when <S, G> is not available for any reason, the stream would typically be flowing when this state exists.

Breaking down each entry in detail:

```
(*, 239.255.255.1)
RP: 192.168.1.1
RPF nbr: 10.132.0.156
RPF idx: port2
```

```
Upstream State: JOINED
Local:
port3
Joined:
Asserted:
FCR:
```

The RP will always be listed in a `*,G` entry, the RPF neighbor and interface index will also be shown. In this topology these are the same in all downstream PIM routers. The state is active so the upstream state is joined.

In this case FGT-3 is the last hop router so the IGMP join is received locally on port3. There is no PIM outgoing interface listed for this entry as it is used for the upstream PIM join.

```
(10.166.0.11, 239.255.255.1)
RPF nbr: 10.132.0.156
RPF idx: port2
SPT bit: 1
Upstream State: JOINED
Local:
Joined:
Asserted:
Outgoing:
port3
```

This is the entry for the SPT, no RP IS listed. The `S,G` stream will be forwarded out of the stated outgoing interface.

```
(10.166.0.11, 239.255.255.1, rpt)
RP: 192.168.1.1
RPF nbr: 10.132.0.156
RPF idx: port2
Upstream State: NOT PRUNED
Local:
Pruned:
Outgoing:
```

The above `S,G,RPT` state is created for all streams that have both a `S,G` and a `*,G` entry on the router. This is not pruned in this case because of the topology, the RP and source are reachable over the same interface.

Although not seen in this scenario, assert states may be seen when multiple PIM routers exist on the same LAN which can lead to more than one upstream router having a valid forwarding state. Assert messages are used to elect a single forwarder from the upstream devices.

Viewing the PIM next-hop table

The PIM next-hop table is also very useful for checking the various states, it can be used to quickly identify the states of multiple multicast streams

```
FGT-3 # get router info multicast pim sparse-mode next-hop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination Type Nexthop Nexthop Nexthop Metric Pref Refcnt
Num Addr Ifindex
_____________________________________________________________
10.166.0.11 ..S. 1 10.132.0.156 9 21 110 3
192.168.1.1 .R.. 1 10.132.0.156 9 111 110 2
```

Viewing the PIM multicast forwarding table

Also you can check the multicast forwarding table showing the ingress and egress ports of the multicast stream.

```
FGT-3 # get router info multicast table

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL threshold)

(10.166.0.11, 239.255.255.1), uptime 04:02:55, stat expires 00:02:25
Owner PIM-SM, Flags: TF
Incoming interface: port2
Outgoing interface list:
port3 (TTL threshold 1)
```

Viewing the kernel forwarding table

Also the kernel forwarding table can be verified, however this should give similar information to the above command:

```
FGT-3 # diag ip multicast mroute
grp=239.255.255.1 src=10.166.0.11 intf=9 flags=(0x10000000)[ ] status=resolved
last_assert=2615136 bytes=1192116 pkt=14538 wrong_if=0 num_ifs=1
index(ttl)=[6(1),]
```

Viewing the multicast routing table (FGT-2)

If you check the output on FGT-2 there are some small differences:

```
FGT-2 # get router info multicast pim sparse-mode table
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 239.255.255.1)
RP: 192.168.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
Local:
Joined:
external
Asserted:
FCR:
```

The `*,G` entry now has a joined interface rather than local because it has received a PIM join from FGT-3 rather than a local IGMP join.

```
(10.166.0.11, 239.255.255.1)
RPF nbr: 10.130.0.237
RPF idx: internal
SPT bit: 1
Upstream State: JOINED
Local:
Joined:
external
```

```
Asserted:
Outgoing:
external
```

The S,G entry shows that we have received a join on the external interface and the stream is being forwarded out of this interface.

```
(10.166.0.11, 239.255.255.1, rpt)
RP: 192.168.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
Local:
Pruned:
Outgoing:
External
```

The S,G,RPT is different from FGT-3 because FGT-2 is the RP, it has pruned back the SPT for the RP to the first hop router.

Viewing the multicast routing table (FGT-1)

FGT-1 again has some differences with regard to the PIM-SM states, there is no *,G entry because it is not in the path of a receiver and the RP.

```
FGT-1_master # get router info multicast pim sparse-mode table
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
```

Below the S,G is the SPT termination because this FortiGate unit is the first hop router, the RPF neighbor always shows as 0.0.0.0 because the source is local to this device. Both the joined and outgoing fields show as external because the PIM join and the stream is egressing on this interface.

```
(10.166.0.11, 239.255.255.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local:
Joined:
external
Asserted:
Outgoing:
external
```

The stream has been pruned back from the RP because the end-to-end SPT is flowing, there is no requirement for the stream to be sent to the RP in this case.

```
(10.166.0.11, 239.255.255.1, rpt)
RP: 0.0.0.0
RPF nbr: 10.130.0.156
RPF idx: external
Upstream State: RPT NOT JOINED
Local:
Pruned:
Outgoing:
```

Example multicast destination NAT (DNAT) configuration

The example topology shown and described below shows how to configure destination NAT (DNAT) for two multicast streams. Both of these streams originate from the same source IP address, which is 10.166.0.11. The example configuration keeps the streams separate by creating 2 multicast NAT policies.

In this example the FortiGate units have the following roles:

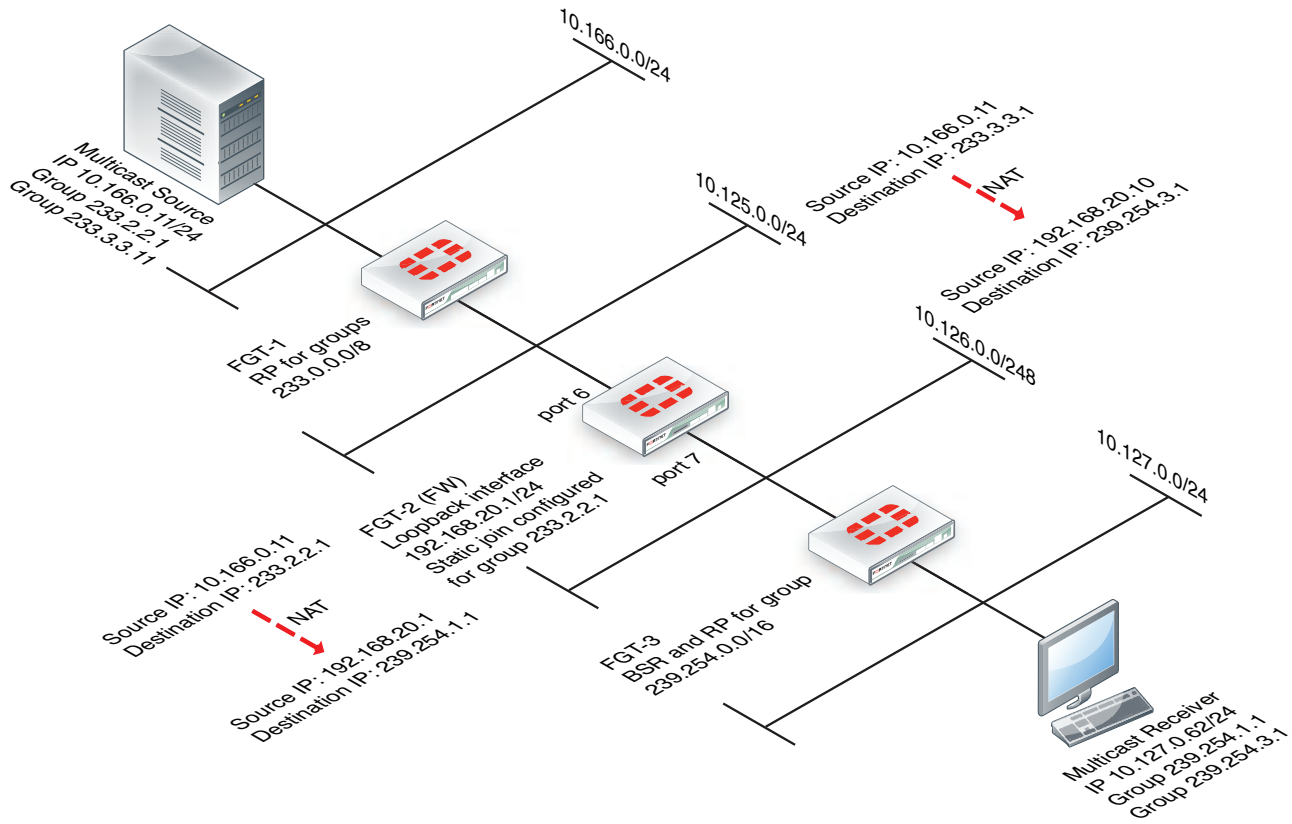
- FGT-1 is the RP for dirty networks, 233.0.0.0/8.
- FGT-2 performs all firewall and DNAT translations.
- FGT-3 is the RP for the clean networks, 239.254.0.0/16.
- FGT-1 and FGT-3 are functioning as PM enabled routers and could be replaced can be any PIM enabled router.

This example only describes the configuration of FGT-2.

FGT-2 performs NAT so that the receivers connected to FGT-3 receive the following translated multicast streams.

- If the multicast source sends multicast packets with a source and destination IP of 10.166.0.11 and 233.2.2.1; FGT-3 translates the source and destination IPs to 192.168.20.1 and 239.254.1.1
- If the multicast source sends multicast packets with a source and destination IP of 10.166.0.11 and 233.3.3.1; FGT-3 translates the source and destination IPs to 192.168.20.10 and 239.254.3.1

Example multicast DNAT topology



To configure FGT-2 for DNAT multicast

1. Add a loopback interface. In the example, the loopback interface is named `loopback`.

```
config system interface
   edit loopback
      set vdom root
      set ip 192.168.20.1 255.255.255.0
      set type loopback
   next
end
```

2. Add PIM and add a unicast routing protocol to the loopback interface as if it was a normal routed interface. Also add static joins to the loopback interface for any groups to be translated.

```
config router multicast
   config interface
      edit loopback
         set pim-mode sparse-mode
            config join-group
               edit 233.2.2.1
               next
               edit 233.3.3.1
               next
            end
      next
```

3. In this example, to add firewall multicast policies, different source IP addresses are required so you must first add an IP pool:

```
config firewall ippool
   edit Multicast_source
      set endip 192.168.20.20
      set interface port6
      set startip 192.168.20.10
   next
end
```

4. Add the translation security policies.

   Policy 2, which is the source NAT policy, uses the actual IP address of port6. Policy 1, the DNAT policy, uses an address from the IP pool. The source and destination addresses will need to be previously created address objects. For this example, 233.3.3.1 255.255.255.255 will be represented by "example-addr_1" and 10.166.0.11 255.255.255.255 will be represented by "example-addr_2". You will likely want to use something more intuitive from your own network.

```
config firewall multicast-policy
   edit 1
      set dnat 239.254.3.1
      set dstaddr example-addr_1
      set dstintf loopback
      set nat 192.168.20.10
      set srcaddr example-addr_2
      set srcintf port6
   next
   edit 2
      set dnat 239.254.1.1
      set dstaddr 233.2.2.1 255.255.255.255
      set dstintf loopback
      set nat 192.168.20.1
```

```
      set srcaddr 10.166.0.11 255.255.255.255
      set srcintf port6
   next
end
```

5. Add a firewall multicast policy to forward the stream from the loopback interface to the physical outbound interface.

   This example is an any/any policy that makes sure traffic accepted by the other multicast policies can exit the FortiGate unit.

```
config firewall multicast-policy
   edit 3
      set dstintf port7
      set srcintf loopback
   next
end
```

Example PIM configuration that uses BSR to find the RP

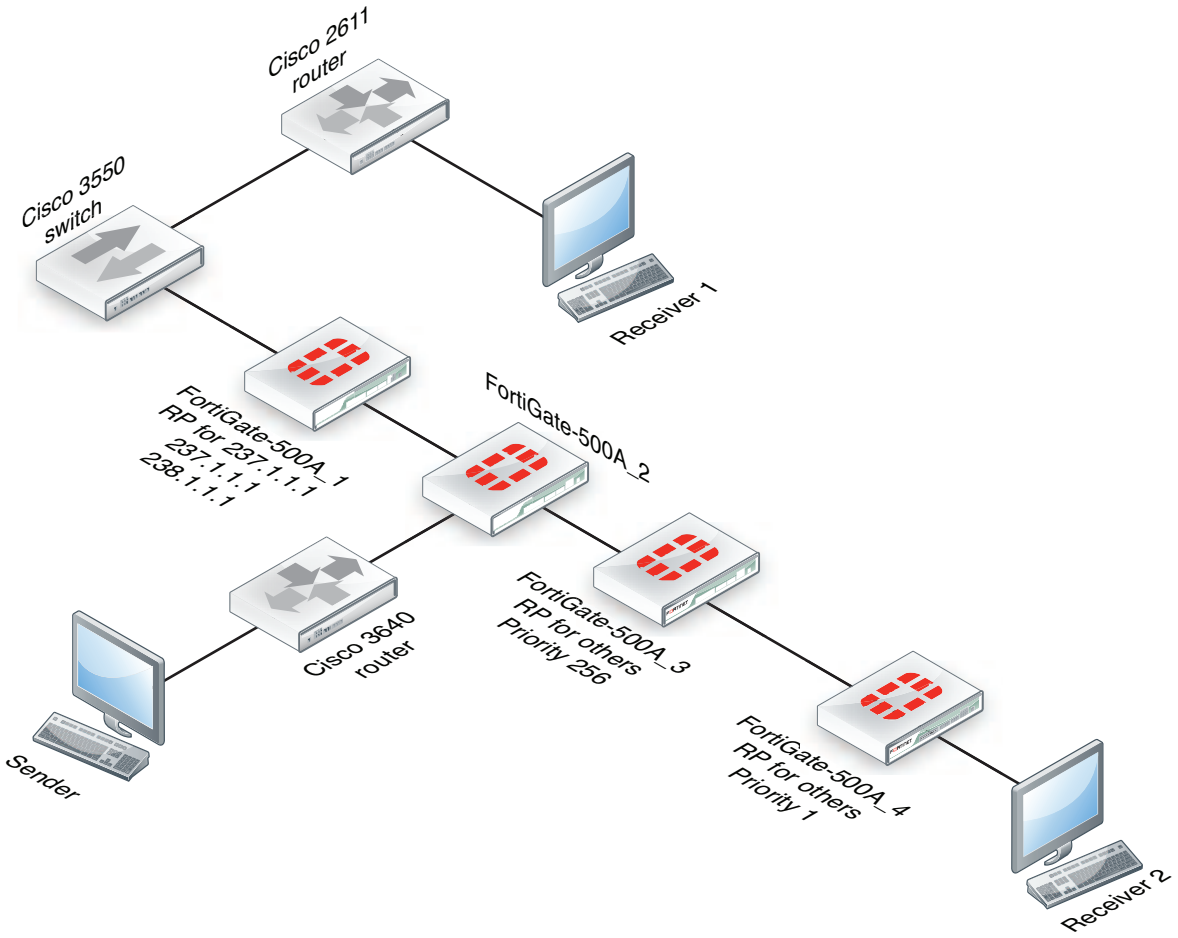
This example shows how to configure a multicast routing network for a network consisting of four FortiGate-500A units (FortiGate-500A_1 to FortiGate-550A_4). A multicast sender is connected to FortiGate-500A_2. FortiGate-500A_2 forwards multicast packets in two directions to reach Receiver 1 and Receiver 2.

The configuration uses a Boot Start Router (BSR) to find the Rendezvous Points (RPs) instead of using static RPs. Under interface configuration, the loopback interface `lo0` must join the 236.1.1.1 group (source).

This example describes:

- Commands used in this example
- Configuration steps
- Example debug commands

PIM network topology using BSR to find the RP



Commands used in this example

This example uses CLI commands for the following configuration settings:

- Adding a loopback interface (lo0)
- Defining the multicast routing
- Adding the NAT multicast policy

Adding a loopback interface (lo0)

Where required, the following command is used to define a loopback interface named `lo0`.

```
config system interface
   edit lo0
      set vdom root
      set ip 1.4.50.4 255.255.255.255
      set allowaccess ping https ssh snmp http telnet
      set type loopback
   next
end
```

Defining the multicast routing

In this example, the following command syntax is used to define multicast routing.

The example uses a Boot Start Router (BSR) to find the Rendezvous Points (RPs) instead of using static RPs. Under interface configuration, the loopback interface `lo0` must join the 236.1.1.1 group (source).

```
config router multicast
   config interface
      edit port6
         set pim-mode sparse-mode
      next
      edit port1
         set pim-mode sparse-mode
      next
      edit lo0
         set pim-mode sparse-mode
         set rp-candidate enable
            config join-group
               edit 236.1.1.1
               next
            end
         set rp-candidate-priority 1
      next
   end
set multicast-routing enable
   config pim-sm-global
      set bsr-allow-quick-refresh enable
      set bsr-candidate enable
      set bsr-interface lo0
      set bsr-priority 200
   end
end
```

Adding the NAT multicast policy

In this example, the incoming multicast policy does the address translation.

The NAT address should be the same as the IP address of the of loopback interface. The DNAT address is the translated address, which should be a new group.

```
config firewall multicast-policy
   edit 1
      set dstintf port6
      set srcintf lo0
   next
   edit 2
      set dnat 238.1.1.1
      set dstintf lo0
      set nat 1.4.50.4
      set srcintf port1
   next
```

Configuration steps

In this sample, FortiGate-500A_1 is the RP for the group 228.1.1.1, 237.1.1.1, 238.1.1.1, and FortiGate-500A_4 is the RP for the other group which has a priority of1. OSPF is used in this example to distribute routes including the loopback interface. All firewalls have full mesh security policies to allow any to any.

- In the FortiGate-500A_1 configuration, the NAT policy translates source address 236.1.1.1 to 237.1.1.1
- In the FortiGate-500A_4, configuration, the NAT policy translates source 236.1.1.1 to 238.1.1.1
- Source 236.1.1.1 is injected into network as well.

The following procedures include the CLI commands for configuring each of the FortiGate units in the example configuration.

To configure FortiGate-500A_1

1. Configure multicast routing.

```
config router multicast
   config interface
      edit port5
         set pim-mode sparse-mode
      next
      edit port4
         set pim-mode sparse-mode
      next
      edit lan
         set pim-mode sparse-mode
      next
      edit port1
         set pim-mode sparse-mode
      next
      edit lo999
         set pim-mode sparse-mode
      next
      edit lo0
         set pim-mode sparse-mode
         set rp-candidate enable
         set rp-candidate-group 1
      next
   end
set multicast-routing enable
   config pim-sm-global
      set bsr-candidate enable
      set bsr-interface lo0
   end
end
```

2. Add multicast security policies.

```
config firewall multicast-policy
   edit 1
      set dstintf port5
      set srcintf port4
   next
   edit 2
      set dstintf port4
      set srcintf port5
   next
```

```
      edit 3
      next
   end
```

3. Add router access lists.

```
   config router access-list
      edit 1
         config rule
            edit 1
               set prefix 228.1.1.1 255.255.255.255
               set exact-match enable
            next
            edit 2
               set prefix 237.1.1.1 255.255.255.255
               set exact-match enable
            next
            edit 3
               set prefix 238.1.1.1 255.255.255.255
               set exact-match enable
            next
         end
      next
   end
```

To configure FortiGate-500A_2

1. Configure multicast routing.

```
   config router multicast
      config interface
         edit "lan"
            set pim-mode sparse-mode
next
edit "port5"
  set pim-mode sparse-mode
            next
            edit "port2"
               set pim-mode sparse-mode
            next
            edit "port4"
               set pim-mode sparse-mode
            next
            edit "lo_5"
               set pim-mode sparse-mode
                  config join-group
                     edit 236.1.1.1
                     next
                  end
               next
            end
         set multicast-routing enable
      end
```

2. Add multicast security policies.

```
   config firewall multicast-policy
      edit 1
         set dstintf lan
```

```
      set srcintf port5
    next
    edit 2
      set dstintf port5
      set srcintf lan
    next
    edit 4
      set dstintf lan
      set srcintf port2
    next
    edit 5
      set dstintf port2
      set srcintf lan
    next
    edit 7
      set dstintf port1
      set srcintf port2
    next
    edit 8
      set dstintf port2
      set srcintf port1
    next
    edit 9
      set dstintf port5
      set srcintf port2
    next
    edit 10
      set dstintf port2
      set srcintf port5
    next
    edit 11
      set dnat 237.1.1.1
      set dstintf lo_5
      set nat 5.5.5.5
      set srcintf port2
    next
    edit 12
      set dstintf lan
      set srcintf lo_5
    next
    edit 13
      set dstintf port1
      set srcintf lo_5
    next
    edit 14
      set dstintf port5
      set srcintf lo_5
    next
    edit 15
      set dstintf port2
      set srcintf lo_5
    next
    edit 16
    next
end
```

To configure FortiGate-500A_3

1. Configure multicast routing.

```
config router multicast
   config interface
      edit port5
         set pim-mode sparse-mode
      next
      edit port6
         set pim-mode sparse-mode
      next
      edit lo0
         set pim-mode sparse-mode
         set rp-candidate enable
         set rp-candidate-priority 255
      next
      edit lan
         set pim-mode sparse-mode
      next
   end
set multicast-routing enable
   config pim-sm-global
      set bsr-candidate enable
      set bsr-interface lo0
   end
end
```

2. Add multicast security policies.

```
config firewall multicast-policy
   edit 1
      set dstintf port5
      set srcintf port6
   next
   edit 2
      set dstintf port6
      set srcintf port5
   next
   edit 3
      set dstintf port6
      set srcintf lan
   next
   edit 4
      set dstintf lan
      set srcintf port6
   next
   edit 5
      set dstintf port5
      set srcintf lan
   next
   edit 6
      set dstintf lan
      set srcintf port5
   next
end
```

To configure FortiGate-500A_4

1. Configure multicast routing.

```
config router multicast
   config interface
      edit port6
         set pim-mode sparse-mode
      next
      edit lan
         set pim-mode sparse-mode
      next
      edit port1
         set pim-mode sparse-mode
      next
      edit lo0
         set pim-mode sparse-mode
         set rp-candidate enable
            config join-group
               edit 236.1.1.1
               next
            end
         set rp-candidate-priority 1
      next
   end
set multicast-routing enable
   config pim-sm-global
set bsr-allow-quick-refresh enable
      set bsr-candidate enable
      set bsr-interface lo0
      set bsr-priority 1
   end
end
```

2. Add multicast security policies.

```
config firewall policy
   edit 1
      set srcintf lan
      set dstintf port6
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 2
      set srcintf port6
      set dstintf lan
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 3
      set srcintf port1
      set dstintf port6
      set srcaddr all
```

```
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 4
      set srcintf port6
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 5
      set srcintf port1
      set dstintf lan
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 6
      set srcintf lan
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 7
      set srcintf port1
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 8
      set srcintf port6
      set dstintf lo0
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 9
      set srcintf port1
      set dstintf lo0
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
```

```
      set service ANY
    next
    edit 10
      set srcintf lan
      set dstintf lo0
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
    next
end
```

Chapter 10 - FortiView

FortiView

This document provides a general guide to FortiView, the FortiOS log view tool, explaining its layout, features, and its usefulness in everyday administrative scenarios.

The following chapters are included in this document:

Overview on page 1 outlines the role FortiView plays in FortiOS and its overall layout. This section also identifies which FortiGate platforms support the full FortiView features.

Sources on page 1 explains the features of FortiView's Sources console, and shows how you can investigate an unusual spike in traffic to determine which user is responsible.

Applications on page 1 explains the features of FortiView's Applications console and shows how you can view what sort of applications their employees are using.

Cloud Applications on page 1 explains the features of FortiView's Cloud Applications console and shows how you can drill down to access detailed data on cloud application usage, e.g. YouTube.

Destinations on page 1 explains the features of FortiView's Destinations console and shows how you can access detailed information on user destination-accessing through the use of drill down functionality.

Web Sites on page 1 explains the features of FortiView's Web Sites console and shows how you can investigate instances of proxy avoidance which is the use of a proxy site in order to access data that might otherwise be blocked by the server.

Threats on page 1 explains the features of FortiView's Threats console and shows how you can monitor threats to the network, both in terms of their Threat Score and Threat Level.

All Sessions on page 1 explains the features of FortiView's All Sessions console and shows how you can filter sessions by port number and application type.

Reference on page 1 explains reference information for the various consoles in FortiView, and describes the assortment of filtering options, drilldown options, and columns available.

Troubleshooting FortiView on page 1 offers solutions to common technical issues experienced by FortiGate users.

Overview

This section provides an overview of FortiView, its interface, and options, including the following:

Enabling FortiView

By default, FortiView is enabled on FortiGates running FortiOS firmware version 5.2 and above. You will find the FortiView consoles under **System > FortiView**. However, certain options will not appear unless the FortiGate has **Disk Logging** enabled.

Only certain FortiGate models support Disk Logging. A complete list of FortiGate platforms that support Disk Logging is provided in the matrix below.

To enable Disk Logging

1. Go to **Log & Report > Log Config > Log Settings** and select the checkbox next to **Disk**.
2. **Apply** the change.

To enable Disk Logging - CLI

```
config log disk setting
   set status enable
end
```

FortiView Feature Support - Platform Matrix

Note that the following table identifies three separate aspects of FortiView in FortiOS 5.2.3:

- Basic feature support
- Historical Data
- Disk Logging

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-20C Series	✔		
FG/FWF-30D/40C Series	✔		
FG/FWF-60C Series	✔		
FG/FWF-60D Series	✔		
FGR-60D	✔		
FG-60D	✔		
FG/FWF-80C Series	✔		
FG-80D	✔	✔	1 hour
FG/FWF-90D Series	✔	✔	1 hour
FG/FWF-92D Series	✔		
FG-110C	✔		
FG-111C	✔	**CLI**	1 hour
FG-100D Series	✔	✔	24 hours
FG-200B Series	✔	**#**	**#** (24 hours)
FG-200D Series	✔	✔	24 hours
FG-310B	✔		**#** (24 hours)
FG-311B	✔		**#** (24 hours)
FG-300C	✔	✔	24 hours
FG-300D	✔	✔	24 hours
FG-500D	✔	✔	24 hours
FG-620B	✔	**#**	**#** (24 hours)
FG-621B	✔	**#**	**#** (24 hours)
FG-600C	✔	✔	24 hours
FG-800C	✔	✔	24 hours

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG-1000C	✔	✔	24 hours
FG-1500D	✔	✔	24 hours
FG-1240B	✔	✔	24 hours
FG-3016B	✔	**#**	**#** (24 hours)
FG-3040B	✔	**CLI**	24 hours
FG-3140B	✔	**CLI**	24 hours
FG-3240C	✔	**CLI**	24 hours
FG-3600C	✔	**CLI**	24 hours
FG-3700D	✔	**CLI**	24 hours
FG-3810A	✔	**#**	**#** (24 hours)
FG-3950B	✔	**#, CLI**	**#** (24 hours)
FG-3951B	✔	**#, CLI**	**#** (24 hours)
FG-5001A	✔	**#, CLI**	**#** (24 hours)
FG-5001B	✔	**CLI**	24 hours
FG-5001C	✔	**CLI**	24 hours
FG-5001D	✔	**CLI**	24 hours
FG-5101C	✔	**CLI**	24 hours
FS-5203B	✔	**CLI**	

✔ = *Default support.*
= *Local storage required.*

* Refer to section on Historical Data below.

Basic feature support

FortiView's consoles give insight into your user's traffic, not merely showing which users are creating the most traffic, but what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

FortiView basic feature support consists of the following consoles:

- Sources
- Applications
- Destinations
- All Sessions

The complete array of features in FortiView requires disk logging enabled (see below). It includes those consoles listed above as well as the following:

- Cloud Applications
- Web Sites
- Threats
- System Events
- Admin Logins
- VPN

Historical Data

Not all FortiView consoles have the same available historical data options, depending on whether or not your traffic is locally stored.

Below is a table showing which features are available for units using local storage, including the historical data options.

Only FortiGate models 100D and above support the 24 hour historical data.

Features	With Local Storage				Without Local Storage			
	Now	5 min	1 hr	24 hr *	Now	5 min	1 hr	24 hr
Sources	✔	✔	✔	✔	✔			
Applications	✔	✔	✔	✔	✔			
Cloud Applications	✔	✔	✔	✔	✔			
Destinations	✔	✔	✔	✔	✔			
Websites	✔	✔	✔	✔				
Threats		✔	✔	✔				
All Sessions	✔	✔	✔	✔	✔			
System Events		✔	✔	✔				
Admin Logins		✔	✔	✔				
VPN		✔	✔	✔				

* Not available for desktop models with SSD.

Disk Logging

Only certain FortiGate models support Disk Logging (see above).

To enable Disk Logging, go to **Log & Report > Log Config > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Configuration Dependencies

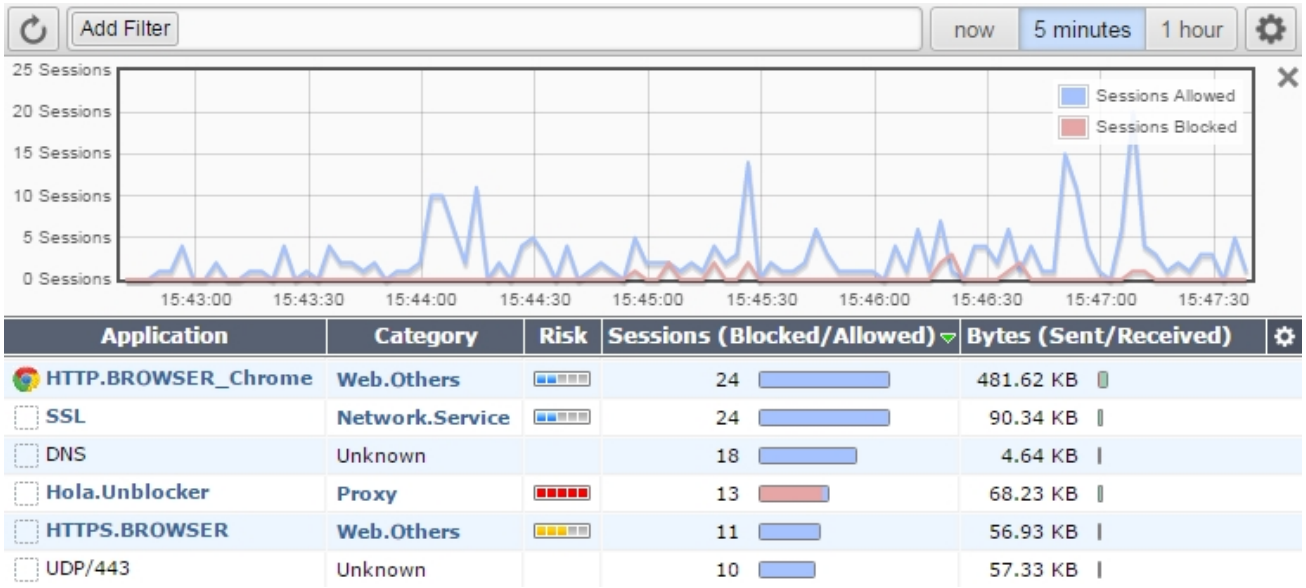
Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

Feature	Dependencies (Realtime)	Dependencies (Historical)
Sources	None, always supported	Disk logging enabled Traffic logging enabled in policy
Applications	None, always supported	Disk logging enabled Traffic logging enabled in policy Application control enabled in policy
Cloud Applications	Not supported	Disk logging enabled Application control enabled in policy SSL "deep inspection" enabled in policy Deep application inspection enabled in application sensor Extended UTM log enabled in application sensor
Destinations	None, always supported	Disk logging enabled Traffic logging enabled in policy
Web Sites	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile
Threats	Not supported	Disk logging enabled Traffic logging enabled in policy Threat weight detection enabled
All Sessions	None, always supported	Disk logging enabled Traffic logging enabled in policy
System Events	Not supported	
Admin Logins	Not supported	
VPN	Not supported	
FortiSandbox	Not supported	

FortiView interface

FortiView lets you access information about the traffic activity on your FortiGate, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:

FortiView Application console sorted by Sessions (Blocked/Allowed)



The top menu bar features a **Refresh** button, which updates the data displayed, a **Filter** button for filtering the data by category, **Time Display** options (now, 5 minutes, 1 hour, or 24 hours), and a **Settings** button (containing additional viewing settings and a link to the Threat Weight menu).

The graph window can be hidden using the **X** in the top right corner, and re-added by selecting **Show Graph**. To zoom in on a particular section of the graph, **click and drag** from one end of the desired section to the other. This will appear in the **Time Display** options as a **Custom** selection. The minimum selection size is 60 seconds.

Only FortiGate models 100D and above support the 24 hour historical data.

FortiView consoles

This section describes the following log filter consoles available in FortiView:

Sources

The **Sources** console provides information about the sources of traffic on your FortiGate unit. This console can be filtered by Destination Interface, Policy, Security Action, Source Device, Source Interface, and Source IP.

Specific devices and time periods can be selected and drilled down for deep inspection.

Scenario: Investigating a spike in traffic

A system administrator notices a spike in traffic and wants to investigate it. From the **Sources** window, they can determine which user is responsible for the spike by following these steps:

1. Go to **System > FortiView > Sources**.
2. In the graph display, click and drag across the peak that represents the spike in traffic.
3. Sort the sources by bandwidth use by selecting the **Bytes (Sent/Received)** header.
4. Drill down into whichever source is associated with the highest amount of bandwidth use by double-clicking it. From this screen, you have an overview of that source's traffic activity.
5. Again, in either the **Applications** or **Destinations** view, select the **Bytes (Sent/Received)** header to sort by bandwidth use.
6. Double-click the top entry to drill down to the final inspection level, from which you can access further details on the application or destination, and/or apply a filter to prohibit or limit access.

Only FortiGate models 100D and above support the 24 hour historical data.

Applications

The **Applications** console provides information about the applications being used on your network. This console can be filtered by Application, Destination Interface, Policy, Security Action, and Source Interface.

Specific devices and time periods can be selected and drilled down for deep inspection.

In order for information to appear in the **Applications** console, Application Control must be enabled in a policy.

Scenario: Viewing application usage

A manager is interested in the office internet habits of their employees:

1. Go to **System > FortiView > Applications**, to view the list of applications accessed by the users on your network. Use the time-frame options to view what applications were used in those time periods (from now, 5 minutes, 1 hour, or 24 hours).
2. From **Sessions (Blocked/Allowed)** and **Bytes (Sent/Received)**, you can see how much traffic has been generated. Click these columns to show the traffic in descending order.
3. You notice that a social media application has created the most traffic of all the applications, and so it's at the top of the list. Drill down into the application by double-clicking, or right-click and select **Drill down to details...**.
4. You are directed to a summary page of the social media application. From here, you can see which specific user has made the most use of the application.

Only FortiGate models 100D and above support the 24 hour historical data.

Cloud Applications

The **Cloud Applications** console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Filed uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: **Applications** and **Users** (located in the top menu bar next to the time periods). **Applications** shows a list of the programs being used. **Users** shows information on the individual users of the cloud applications, including the username, if the FortiGate was able to view the login event.

This console can be filtered by Cloud Application.

In order for information to appear in the **Cloud Applications** console, an application control profile (that has Deep Inspection of Cloud Applications turned on) must be enabled in a policy, and SSL Inspection must use `deep-inspection`.

Scenario: Viewing cloud application usage data

From the Cloud Applications console, users can drill down to access detailed data on cloud application usage data. In this scenario, the console is used to determine the network's most frequent user of YouTube over a 24-hour period, and find out more about their usage patterns.

1. Go to **System > FortiView > Destinations**.
2. Select **Applications** view from the top menu bar if it is not already selected.
3. Select **24 Hours** from the Time Display options.
4. Find **YouTube** under the Application column and double-click it (or right-click and select **Drill down for details...**). This will open the YouTube stats window.

5. To determine the user who has accessed YouTube the most frequently, sort the column entries by **Sessions** by selecting the column header of the same name.
6. Double-click (or right-click and select **Drill down for details...**) the top-bandwidth YouTube user to view detailed stats, including the names of videos watched by the user and the date and time each video was accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Destinations

The **Destinations** console provides information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, and also select the device and time period, and apply search filters.

This console can be filtered by Destination Interface, Destination IP, Policy, Security Action, and Source Interface.

Scenario: Monitoring destination data

The Destinations console can be used to access detailed information on user destination-accessing through the use of the console's drilldown functionality. In this scenario, the console is used to find out more about a particular user's Facebook usage patterns over a 24-hour period:

1. Go to **System > FortiView > Destinations**.
2. Select **1 hour** from the Time Display options at the top right corner of the console.
3. The easiest way to locate most destinations is to scan the Applications column for the name of the application. Once the session containing Facebook has been located, double-click it to access the Destination summary window.
4. Locate Facebook in the Applications column and double-click it to view the Facebook drilldown page. From here, detailed information regarding the user's Facebook session can be accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Web Sites

The **Web Sites** console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

This dashboard can be filtered by Domain.

In order for information to appear in the **Web Sites** console, web filtering must be enabled in a policy, with FortiGate Categories enabled.

Scenario: Investigating an instance of Proxy Avoidance

In this scenario, the Categories view will be used to investigate an instance of Proxy Avoidance, one of the Categories recognized by FortiOS. Proxy Avoidance denotes the use of a proxy site in order to access data that might otherwise be blocked by the server.

1. Go to **System > FortiView > Web Sites** to open the Web Sites console.
2. Select **Categories** from the top bar menu to enter Categories view.
3. Scan the **Categories** column and locate the instance of Proxy Avoidance, then double-click it to enter its drill down screen.

Only FortiGate models 100D and above support the 24 hour historical data.

Threats

The **Threats** console lists the top users involved in incidents, as well as information on the top threats to your network.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

The console can be filtered by Destination Interface, Policy, Security Action, Source Interface, Threat, and Threat Type.

In order for information to appear in the **Threats** console, Threat Weight Tracking must be enabled.

Scenario: Monitoring Threats to the Network

Some users have high Threat Scores. The Threats console can be used to view all threats and discover why such high scores are being shown:

1. In the graph display, click and drag across the peak that represents the spike in threat score.
2. Sort the threats by score or level by selecting the **Threat Score (Blocked/Allowed** or the **Threat Level** headers respectively.
3. You see that a specific threat's Threat Level is at Critical. Drill down into the threat by double-clicking, or right-click and select **Drill down to details...**.
4. From this summary page, you can view the source IPs and the number of sessions that came from this threat. Double-click on one of them.
5. The following page shows a variety of statistics, including **Reference**. The URL next to it will link you to a FortiGuard page where it will display the description, affected products, and recommended actions, if you are not familiar with the particular threat.

Only FortiGate models 100D and above support the 24 hour historical data.

All Sessions

The **All Sessions** console provides information about all FortiGate traffic. This console can be filtered by Application, Checksum, Destination Interface, Destination IP, Policy, Security Action, Source Device, Source Interface, Source IP, Threat, and Threat Type.

This console has the greatest number of column options to choose from. To choose which columns you wish to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

A number of columns available in FortiView are only available in All Sessions. For example, the **Action** column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the **Source**, **Destination**, and **Bytes (Sent/Received)** columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is **Protocol**. This allows you to display the protocol type associated with the selected session, e.g. TCP, FTP, HTTP, HTTPS, and so on.

Scenario: Filtering sessions by port number and application type

From the **All Sessions** console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.

1. Go to **System > FortiView > All Sessions**.
2. Select **now** from the **Time Display** options if it is not already selected.
3. Select the **Filter** button, then select **Applications**. This will open a drop-down menu listing the applications that appear in the master session list. From this list, locate and select **Skype**, or type `Skype` into the search bar and hit **Enter**. This will filter the session list to only feature Skype usage.
4. Select the **Filter** button again, then select **Destination Port** from the drop-down menu, then locate and select the desired port number. This will add a second filter which will restrict the results to presenting only the Skype data associated with that port number.

Only FortiGate models 100D and above support the 24 hour historical data.

System Events

The **System Events** console lists security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level (**Alert**, **Critical**, **Emergency**, **Error**, or **Warning**), and the number of instances the events were detected. This console can be filtered by Event Name and Severity.

Scenario: Viewing Security Events & Security Actions

System Events can be used in conjunction with All Sessions to see what network security events took place, and specifically see what action was taken upon their detection:

- Go to **System > FortiView > System Events**, to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
- You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Note when the event took place, and go to **System > FortiView > All Sessions**, to see more information pertaining to the security event.
- From this console, you can determine the system event's source, how much traffic was sent and received, and the security action taken in response to this security event. These actions differ, depending upon the severity of the security event. To view these actions, see the table-entry for **Security Action** in Columns displayed on page 1139.

Only FortiGate models 100D and above support the 24 hour historical data.

Admin Logins

The **Admin Logins** console provides information on administrator interactions with the network, including the number of login instances, number of failed logins, and the length of time logged in. This console can be filtered by User Name.

Scenario: Scrutinizing Administrator Security

Admin Logins can be used in conjunction with System Events to see who was on during a system change that impacted performance and allowed a threat to persist/pass through the firewall:

- Go to **System > FortiView > System Events**, to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
- You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Double-click on the event to drill down.
- Once drilled down, you can see the date and time that the system change took place.
- Go to **System > FortiView > Admin Logins**, to see who has been logged in, how long they have been logged in, and what configuration changes they have made. Using the time graph, you can correlate the information from System Events with who was logged in at the time the threat was allowed.

Only FortiGate models 100D and above support the 24 hour historical data.

VPN

From the **VPN** console, users can access information on any VPNs associated with their FortiGate. From the initial window, a list of all the associated VPNs is provided, along with general information, such as number of user connections and VPN type. By double-clicking on an individual VPN (or right-clicking and selecting **Drill down for details...**), users can access more specific data on that VPN.

Logs in the VPN console can be sorted by number of connections, last connection time, or data sent/received by selecting the column headers.

This console can be filtered by User Name and VPN Type.

Certain dashboard options will not appear unless your FortiGate has Disk Logging enabled.

Furthermore, only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 1121 for more information.

To enable Disk Logging, go to **Log & Report > Log Config > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Scenario: Investigating VPN user activity

The VPN console can be used to access detailed data on VPN-user activity via the use of the drill down windows. In this scenario, the administrator looks into the usage patterns of the IPsec user who has most frequently connected to the network.

1. Go to **System > FortiView > VPN** to view the VPN console.
2. Select the **Connections** column header to sort the entries by number of connections to the network.
3. Locate the top user whose VPN Type is **ipsec** and double-click the entry to enter that user's drill down screen.
4. To get the most representative data possible, sort the entries by bandwidth use by selecting the **Bytes (Sent/Received)** column header. Double-click the top entry to enter the drill down window for that connection instance.
   From this screen, the administrator can find out more about the specific session, including the date/time of access, the XAuth (Extensible Authentication) User ID, the session's Tunnel ID, and more.

Reference

This section consists of reference information for the various consoles in FortiView. Each console has an assortment of filtering options, drilldown options, and columns that can be displayed. Since many of these options and columns persist through each console, the entire list of options and their descriptions is included below. Attempts have been made to identify the instances where an option or column is only available to a particular console.

This section includes:

Filtering options

When you select the **Add Filter** button, a drop-down list appears with a list of available filtering options. Available options differ based on which console is currently being viewed. The following table explains all of the available filtering options:

Filter option	Description
Application	Filter by application name.
Checksum	Filter by checksum value. Checksums are reference digits used to represent the correct datasum of a packet in order to detect errors.
Cloud Application	Filter by cloud application name. **Note:** This filter is only available in the **Cloud Applications** console.
Destination Interface	Filter by the interface type used by the destination user, e.g. wan1.
Destination IP	Filter by the IP address used by the destination.
Destination Port	Filter by the port used by the destination. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Domain	Filter by domain name. **Note:** This filter is only available in the **Web Sites** console.
Event Name	Filter by security event name. **Note:** This filter is only available in the **System Events** console.
File Name	Filter by file name. **Note:** This filter is only available in the **FortiSandbox** console.
NAT Source IP	Filter by the NAT-translated source IP address. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
NAT Source Port	Filter by the NAT-translated source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Policy	Filter by the policy identification number.
Protocol	Filter by the protocol used by the source, e.g. tcp or udp. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).

Filter option	Description
Security Action	Filter by the type of response taken to the security event. The types of possible actions are as follows: **Allowed:** No threat was detected and the connection was let through. **Blocked:** A threat was detected and the connection was not let through. **Reset:** A possible issue was detected and the connection was reset. **Traffic Shape:** Some data packets may have been delayed to improve system-wide performance.
Severity	Filter by the severity level (**Critical**, **High**, **Medium** or **Low**) associated with a security event.
Source Device	Filter by source device type, e.g. mobile.
Source Interface	Filer by the interface type used by the source user, e.g. wan1.
Source IP	Filter by the source IP address.
Source Port	Filter by the source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Status	Filter by the maliciousness of a file. The types of possible status' are **Malicious**, **High**, **Medium**, **Low**, **Clean**, **Unknown**, and **Pending**. **Note:** This filter is only available in the **FortiSandbox** console.
Threat	Filter by threats received.
Threat Type	Filter by threat classification, e.g. DoS.
User Name	Filter by user name.
VPN Type	Filter by Virtual Private Network (VPN) protocol type, e.g. PPTP. **Note:** This filter is only available in the **VPN** console.

Drilldown options

Double-click, or right-click, on any entry in a FortiView console and select **Drill down to details...**, to view the following tabs (options vary depending on the console selected):

Drilldown option	Description
Applications	Select to drill down by application to view application-related information, including the application name, sessions blocked and allowed, bytes sent and received, and the risk level. You can sort entries by selecting the column header.
Destinations	Select to drill down by destination to view destination-related information, including the IP address and geographic region, interface, threat score, number of sessions blocked and allowed, and bytes sent and received. You can sort entries by selecting the column header.
Threats	Select to drill down by threat to view threat-related information, including the threat name, category, threat level, threat score, and number of sessions blocked and allowed. You can sort entries by selecting the column header.
Domains	Select to drill down by domain to view domain-related information, including domain name, category, browsing time, threat weight, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
Categories	Select to drill down by category to view category-related information, including category name, browsing time, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
Sessions	Select to drill down by sessions to view session-related information, including date/time, source, destination IP address and geographic region, application name,security action, security event, and bytes sent/received. You can sort entries by selecting the column header.
Sources	Select to drill down by rows to view source-related information, including IP address, device type, interface type, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.

Columns displayed

The following columns appear in the initial window of the consoles. Some columns may only be visible by selecting them from the column drop-down menu. Options also vary depending on the console selected.

Column name	Description
Action	Displays the type of response taken to a security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance. **Note:** This column is only available in the **All Sessions** console.
Application	Displays the application name and service. When **Time Display** is set to **now**, you can access further information about an application by selecting the column entry.
Application Category	Displays the type of application used in the selected session, e.g. video player, social media. **Note:** This column is only available in the **All Sessions** console.
Application ID	Displays the identification number associated with the application used in the selected session. **Note:**This column is only available in the **All Sessions** console.
Application Risk **Risk**	Displays the application risk level. You can hover the mouse cursor over the entry in the column for additional information, and select the column header to sort entries by level of risk. Risk uses a 5-point risk rating. The rating system is as follows: • **Critical**: Applications that are used to conceal activity to evade detection. • **High**: Applications that can cause data leakage, are prone to vulnerabilities, or may download malware. • **Medium**: Applications that can be misused. • **Elevated**: Applications that are used for personal communications or can lower productivity. • **Low**: Business-related applications or other harmless applications.

Column name	Description
Browsing Time	Displays the amount of time a user has spent browsing a web site (in seconds). **Note:** This column is only available in the **Web Sites** console, in **Categories** view..
Bytes (Sent/Received)	Displays the size of sent and received data packets, as measured in bytes. Select the column header to sort the entries by size. **Note:** This information is available on some consoles as two separate columns: **Sent** and **Received**.
Category	Displays the category descriptor appropriate to whatever console is being displayed. For example, threat categories are displayed in the Threats console.
Clean	Displays the number of "clean" (safe) files found in the selected FortiSandbox session. **Note:** This column is only available in the **FortiSandbox** console, in **Source** view.
Cloud User	Displays the users accessing cloud applications by IP address. **Note:** This column is only available in the **Cloud Applications** console, in **Users** view.
Configuration Changes	Displays the number of configuration changes made by the user. You can hover the mouse cursor over an entry for additional information. **Note:** This column is only available in the **Admin Logins** console.
Connections	Displays the number of VPN connections made by the selected user.. **Note:** This column is only available in the **VPN** console.
Destination	Displays the destination name, IP address and geographic region.
Destination Country	Displays the country session data is being sent to. **Note:** This column is only available in the **All Sessions** console.
Destination Interface	Displays which interface session data is being sent through, e.g. wan1.
Destination Port	Displays the port number of the destination server being used to accept data. Note: This column is only available in the **All Sessions** console.

Column name	Description
Device	Displays the device IP address or Fully Qualified Domain Name (FQDN).
Domain	Displays the domain associated with the selected web site, e.g. google.-com. **Note:** This column is only available in the **Web Sites** console.
DST Nat IP **NAT Destination**	Displays the Network Address Translation (NAT) IP address associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
DST Nat Port **NAT Destination Port**	Displays the Network Address Translation (NAT) port number associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
Duration	Displays the amount of time (in seconds) a user has been logged in. **Note:** This column is only available in the **Admin Logins** console.
Event Name (Description)	Displays the name and description of the selected security event. **Note:** This column is only available in the **System Events** console.
Events	Displays the number of security events that occurred within a selected session. **Note**: This column is only available in the **System Events** console.
Expires	Displays the amount of time a session has (in seconds) before it is set to expire. **Note:** This column is only available in the **All Sessions** console, in **now** Time Display view.
Failed Logins	Displays the number of failed login attempts made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Files (Up/Down)	Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information. **Note:** This column is only available in the **Cloud Applications** console.

Column name	Description
FortiASIC	Displays the type of FortiASIC hardware acceleration used in the specified session, if present. **Note:** This column is only available in the **All Sessions** console, in the **now** Time Display view.
Group	Displays the group ID associated with the selected session. **Note:** This column is only available in the **All Sessions** console.
Last Connection Time	Displays the most recent instance of connection to the selected Virtual Private Network (VPN). **Note:** This column is only available in the **VPN** console.
Level **Threat Level**	Displays the threat level. Select the column header to sort entries by threat level.
Log ID	Displays the identification number for the data log associated with this entry. **Note:** This column is only available in the **All Sessions** console.
Login IDs	Displays the number of login IDs associated with the selected cloud application. **Note:** This column is only available in the **Cloud Applications** console, in **Applications** view.
Logins	Displays the number of successful logins made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Policy ID	Displays the identification number of the policy under which the selected connection was allowed.
Policy UUID	Displays the Universally Unique Identifier (UUID) of the selected policy, if present. **Note:** This column is only available in the **All Sessions** console.
Protocol	Displays the protocol type associated with the selected session, e.g. TCP. **Note:** This column is only available in the **All Sessions** console.

Column name	Description
Security Action	Displays the action taken in response to the selected security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance.
Security Events	Displays the type of security event detected in the selected session. **Note**: This column only appears in the **All Sessions** console.
Sequence Number	Displays the TCP sequence number associated with the selected session. **Note**: This column only appears in the **All Sessions** console.
Service	Displays the ID of the service application in use in the selected session. **Note:** This column only appears in the **All Sessions** console.
Sessions	Displays the number of sessions associated with the selected destination. **Note:** This column only appears in the **Destinations** console, in the **now** Time Display view.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed by FortiOs. In some consoles, entries can be sorted by number of sessions by selecting the column header..
Severity	Displays the severity level (**Critical**, **High**, **Medium** or **Low**) associated with the selected security event. **Note:** This column is only available in the **System Events** console.
Source	Displays the source IP address and/or user ID, if applicable.
Source Interface	Displays which interface is being used by the destination server (eg. wan1).
Source Port	Displays the port number being used by the source server to send data.
Src NAT IP **NAT Source**	Displays the Network Address Translation (NAT) IP address associated with the source server.

Column name	Description
Src NAT Port **NAT Source Port**	Displays the Network Address Translation (NAT) port number associated with the source server.
Status	Displays the status of **Note:** This column is only available in the **FortiSandbox** console, in **Files** view.
Submittted	Displays the number of files submitted to the FortiSandbox for assessment in the selected session. **Note:** This column is only available in the **FortiSandbox** console, in **Files** view.
Threat	Displays the threat type detected in the selected session.
Threat Score (Blocked/Allowed)	Displays the threat score value, a measurement of the total number of threats detected over the course of the session. You can select the column header to sort entries by threat score.
Threat Weight	Displays the threat weight profile associated with the selected session.
Timestamp	Displays the selected session's PHP timestamp.
User **User Name**	Displays the user name associated with the selected administrator.
Videos Played	Displays the number of videos played via cloud applications. **Note:** This column is only available in the **Cloud Applications** console.
VPN	Displays the Virtual Private Networks (VPNs) connected to the FortiGate, by name. **Note:** This column is only available in the **All Sessions** console.
VPN Type	Displays the type of VPN protocol (eg. PPTP, L2TP) in use by the associated connection.

Risk level indicators

There are currently two consoles within FortiView that display the Risk associated with the console: Applications and Cloud Applications. Each application pose different levels of risk to the network, represented by a colour code.

The following table identifies each risk level, from least to most severe:

Indicator	Risk	Description
	Green: *Risk Level 1*	These applications have little to no risk level, with no assigned risk definition. Application file-sharing may result in data leakage, which would be a typical example of a low level risk. An example application would be the Google toolbar, or Dropbox.
	Blue: *Risk Level 2*	These applications have an elevated risk level and typically use excessive bandwidth. High bandwidth consumption can lead to increased operational costs. An example application would be Bittorrent.
	Yellow: *Risk Level 3*	These applications have a low risk level and are typically evasive. Evasive applications can lead to compliance risks, and could include applications such as JustinTV and GlypeProxy.
	Orange: *Risk Level 4*	These applications have a high risk level, and are defined as using both excessive and evasive bandwidth. Example applications would be AutoHideIP and PandoraTV.
	Red: *Risk Level 5*	Applications that have a high risk level are prone to malware or vulnerabilities that can introduce business continuity risks.

Troubleshooting FortiView

FortiView does not display all consoles listed in this document

Some consoles require disk logging to be enabled before they will appear in FortiView. These include:

- Admin Logins
- Cloud Applications
- FortiSandbox
- Sources
- System Events
- Threats
- VPN
- Web Sites

Only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 1121 for more information.

No logging data is displayed

In order for information to appear in the FortiView consoles, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Config > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

```
config log disk setting
   set status enable
end
```

Only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 1121 for more information.

Chapter 11 - Hardening

Hardening your FortiGate

This document describes a series of techniques used to improve the security of administrative access to a FortiGate device.

The following sections are included:

Install the FortiGate unit in a physically secure location
Maintain the firmware
Add new administrator accounts
Change the admin account name and limit access to this account
Only allow administrative access to the external interface when needed
When enabling remote access, configure Trusted Hosts and Two-factor Authentication
Change the default administrative port to a non-standard port
Modify the device name
Register with support services
Maintain short login timeouts
Enable automatic clock synchronization
Enable Password Policy
Modify administrator account Lockout Duration and Threshold values
Disable auto installation via USB
Configure auditing and logging

Install the FortiGate unit in a physically secure location

A good place to start with is physical security. Install the FortiGate unit in a secure location, such as a locked room or a room with restricted access. This way unauthorized users can't get physical access to the device.

If unauthorized users have physical access they can disrupt your entire network by disconnecting your FortiGate unit (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

Maintain the firmware

On installation of a new firewall, it is necessary to update the firmware to the latest version provided by the manufacturer.

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the Release Notes for a new firmware release.
- Review the Supported Upgrade Paths document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration, including local certificates.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Add new administrator accounts

Rather than allowing all administrators to access the FortiGate unit with the admin administrator account you should create administrator accounts for each person that requires administrative access. That way you can track who has made configuration changes and performed other administrative activities. Keep the number of administrative accounts to a minimum to keep better control on who can access the device.

To add administrators go to **System > Admin > Administrators** and select **Create New**.

If you want administrators to have access to all FortiGate configuration options, their accounts should have the **prof_admin** admin profile. Administrators with this profile can do anything except add new administrator accounts.

At least one account should always have the **super_admin** profile as this profile is required to add and remove administrators. To improve security only a very few administrators (usually one) should be able to add new administrators.

If you want some administrator accounts to have limited access to the FortiGate configuration you can create custom admin profiles that only allow access to selected parts of the configuration. To add custom admin profiles, go to **System > Admin > Admin Profiles** and select **Create New**.

For example, if you want to add an admin profile that does not allow changing firewall policies, when you configure the admin profile set **Firewall Configuration** to **None** or **Read Only**.

Change the admin account name and limit access to this account

The default super_admin administrator account, admin, is a well known administrator name so if this account is available it could be easier for attackers to access the FortiGate unit because they know they can log in with this name, only having to determine the password. You can improve security by changing this name to one more difficult for an attacker to guess.

To do this, create a new administrator account with the super_admin admin profile and log in as that administrator. Then go to **System > Admin > Administrators** and edit the admin administrator and change the Administrator name.

Once the account has been renamed you could delete the super_admin account that you just added. Consider also only using the super-admin account for adding or changing administrators. The less this account is used to less likely that it could be compromised. You could also store the account name and password for this account in a secure location in case for some reason the account name or password is forgotten.

Only allow administrative access to the external interface when needed

When possible, don't allow administration access on the external interface and use internal access methods such as IPsec VPN or SSL VPN.

To disable administrative access on the external interface, go to **System > Network > Interfaces,** edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under **Administrative Access.**

This can also be done with CLI using following commands:

```
config system interface
   edit <external_interface_name>
   unset allowaccess
end
```

Please note that this will disable all services on the external interface including CAPWAP, FMG-Access, SNMP, and FCT-Access. If you need some of these services enabled on your external interface, for example CAPWAP and FMG-Access to ensure connectivity between FortiGate unit and respectively FortiAP and FortiManager, then you need to use following CLI command:

```
config system interface
   edit <external_interface_name>
   set allowaccess capwap fgfm
end
```

When enabling remote access, configure Trusted Hosts and Two-factor Authentication

If you have to have remote access and can't use IPsec or SSL VPN then you should only allow HTTPS and SSH and use secure access methods such as trusted hosts and Two-factor authentication.

Configuring Trusted Hosts

Setting trusted hosts for administrators limits what computers an administrator can log in the FortiGate unit from. When you identify a trusted host, the FortiGate unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet will be dropped. To ensure the administrator has access from different locations, you can enter up to ten IP addresses or subnets. Ideally, this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields.

Trusted hosts are configured when adding a new administrator by going to **System > Admin > Administrators** in the web-based manager and selecting **Restrict this Admin Login from Trusted Hosts Only**, or `config system admin` in the CLI.

The trusted hosts apply to the web-based manager, ping, snmp and the CLI when accessed through SSH. CLI access through the console port is not affected.

Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

Configuring Two-factor Authentication

FortiOS 5.0 provides support for FortiToken and FortiToken Mobile. FortiToken Mobile is a Fortinet application that enables you to generate One Time Passwords (OTPs) on a mobile device for FortiGate two-factor authentication. The user's mobile device and the FortiGate unit must be connected to the Internet to activate FortiToken mobile. Once activated, users can generate OTPs on their mobile device without having network

access. FortiToken Mobile is available for iOS and Android devices from their respective Application stores. No cellular network is required for activation.

The latest FortiToken Mobile documentation is available from the FortiToken page of the Fortinet Technical Documentation website.

Two free trial tokens are included with every registered FortiGate unit. Additional tokens can be purchased from your reseller or from Fortinet.

To assign a token to an administrator go to **System > Admin > Administrators** and either add a new or select an existing administrator to assign the token to. Configure the administrator as required, you need to enter your email address and phone number in order to receive the activation code for the FortiToken mobile. Select **Enable Two-factor Authentication**. Select the token to associate with the administrator. Select **OK** to assign the token to the administrator.

To configure your FortiGate unit to send email or SMS messages go to **System > Config > Advanced > Email Service** or **System > Config > Advanced > SMS Service**.

Change the default administrative port to a non-standard port

Administration Settings under **System > Admin > Settings** or `config system global` in the CLI, enable you to change the default port configurations for administrative connections to the FortiGate unit for added security. When connecting to the FortiGate unit when the port has changed, the port must be included. For example, if you are connecting to the FortiGate unit using HTTPS over port 8081, the URL would be `https://192.168.1.99:8081`

If you make a change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is not used for other services.

Modify the device name

The name of the device needs to be modified in order for it to be perfectly identified. A label shall also be placed with the device name. Finally it shall be necessary to add an entry in the DNS with the name of the unit and its IP address.

Register with support services

In order to activate the services and warranty of the device, it is necessary to register the serial number of the device in the manufacturer's website. This task shall always be performed with the same account under which all units have been registered, in order to obtain centralized management.

Maintain short login timeouts

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out. That is, if the web-based manager is not used for a specified amount of time, the FortiGate unit will automatically log the administrator out. To continue their work, they must log in again.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out, go to **System > Admin > Settings** and enter the amount of time for the Idle Timeout. A best practice is to keep the default of 5 min.

When logging into the console using SSH, the default time of inactivity to successfully log into the FortiGate unit is 120 seconds (2 minutes). You can configure the time to be shorter by using the CLI to change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds. To set the logout time enter the following CLI commands:

```
config system global
   set admin-ssh-grace-time <number_of_seconds>
end
```

Enable automatic clock synchronization

Maintain the clock in the device synchronized with the rest of the devices in the network. This facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols.

In Global configuration mode (`Config Global`), execute:

```
config system ntp
      config ntpserver
         edit 1
            set server "192.0.2.1"
         next
      end
   set ntpsync enable
   set syncinterval 60
end
```

Enable Password Policy

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if “p4ssw0rd” is used as a password, it can be cracked.

Password policies, available by going to **System > Admin > Settings > Enable Password Policy**, enable you to create a password policy that any administrator who updates their passwords, must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time frame. The FortiGate unit will warn of any password that is added and does not meet the criteria.

Modify administrator account Lockout Duration and Threshold values

Account lockout policies control how and when accounts are locked out of the FortiGate unit. These policies are described and implemented as follows:

Administrator account Lockout Duration

If someone violates the lockout controls by entering an incorrect user name and/or password, account lockout duration sets the length of time the account is locked. the lockout duration can be set to a specific length of time using a value between 1 and 4294967295 seconds. The default value is 60 seconds.

When it’s required use the CLI to modify the lockout duration as follow:

```
config system global
   set admin-lockout-duration <integer>
end
```

Administrator account Lockout Threshold

The lockout threshold sets the number of invalid logon attempts that are allowed before an account is locked out. You may set a value that balances the need to prevent account cracking against the needs of an administrator who may have difficulty accessing their account.

Its normal for an administrator to sometimes take a few attempts to logon with the right password.

The lockout threshold can be set to any value from 1 to 10. The Default value is 3, which is normally a good setting. However, to improve security you could reduce it to 1 or 2 as long as administrators know to take extra care when entering their passwords.

Use the following CLI command to modify the lockout threshold:

```
config system global
   set admin-lockout-threshold <integer>
end
```

Keep in mind that the higher the lockout value, the higher the risk that someone may be able to break into the FortiGate unit.

Disable auto installation via USB

An attacker with a physical access to the device could load a new configuration or firmware on the FortiGate using the USB port, reinitializing the device through a power cut. To avoid this, execute the following CLI commands:

```
config system auto-install
   set auto-install-config disable
   set auto-install-image disable
end
```

Configure auditing and logging

Audit web facing administration interfaces. By default, FortiGate logs all deny actions. You can check these actions by going to **Log & Report > Event Log > System**. This default behavior should not be changed. Also secure log files in a central location such as FortiCloud and configure alert email which provides an efficient and direct method of notifying an administrator of events. You can configure log settings by going to **Log & Report** > **Log Config**.

An auditing schedule should be established to routinely inspect logs for signs of intrusion and probing.

Chapter 12 - Hardware Acceleration

This FortiOS Handbook chapter contains the following sections:

Hardware acceleration overview describes the capabilities of FortiGate content processors (CPs), security processors (SPs) and network processors (NPs). This chapter also describes how to determine the hardware acceleration components installed in your FortiGate unit and contains some configuration details and examples.

NP6 Acceleration describes the FortiGate NP6 network processor.

FortiGate NP6 architectures contains details about the network processing architectures of FortiGate units that contain NP6 processors.

NP4 Acceleration describes the FortiGate NP4 network processor.

FortiGate NP4 architectures contains details about the network processing architectures of FortiGate units that contain NP4 processors.

Hardware acceleration overview

Most FortiGate models have specialized acceleration hardware that can offload resource intensive processing from main processing (CPU) resources. Most FortiGate units include specialized content processors (CPs) that accelerate a wide range of important security processes such as virus scanning, attack detection, encryption and decryption. (Only selected entry-level FortiGate models do not include a CP processor.) Many FortiGate models also contain security processors (SPs) that accelerate processing for specific security features such as IPS and network processors (NPs) that offload processing of high volume network traffic.

Content processors (CP4, CP5, CP6 and CP8)

Most FortiGate models contain FortiASIC Content Processors (CPs) that accelerate many common resource intensive security related processes. CPs work at the system level with tasks being offloaded to them as determined by the main CPU. Capabilities of the CPs vary by model. Newer FortiGate units include CP8 processors. Older CP versions still in use in currently operating FortiGate models include the CP4, CP5, and CP6.

CP8 capabilities

The CP8 content processor provides the following services:

- IPS signature matching acceleration
- High performance VPN bulk data engine
  - IPsec and SSL/TLS protocol processor
  - DES/3DES/AES in accordance with FIPS46-3/FIPS81/FIPS197
  - ARC4 in compliance with RC4
  - MD5/SHA-1/SHA256 with RFC1321 and FIPS180
  - HMAC in accordance with RFC2104/2403/2404 and FIPS198
- Key Exchange Processor support high performance IKE and RSA computation
  - Public key exponentiation engine with hardware CRT support
  - Primarily checking for RSA key generation
  - Handshake accelerator with automatic key material generation
  - Random Number generator compliance with ANSI X9.31
  - Sub public key engine (PKCE) to support up to 4096 bit operation directly
- Message authentication module offers high performance cryptographic engine for calculating SHA256/SHA1/MD5 of data up to 4G bytes (used by many applications)
- PCI express Gen 2 four lanes interface
- Cascade Interface for chip expansion

CP6 capabilities

- Dual content processors
- FIPS-compliant DES/3DES/AES encryption and decryption
- SHA-1 and MD5 HMAC with RFC1321 and FIPS180
- HMAC in accordance with RFC2104/2403/2404 and FIPS198
- IPsec protocol processor

- High performance IPsec engine
- Random Number generator compliance with ANSI X9.31
- Key exchange processor for high performance IKE and RSA computation
- Script Processor
- SSL/TLS protocol processor for SSL content scanning and SSL acceleration

CP5 capabilities

- FIPS-compliant DES/3DES/AES encryption and decryption
- SHA-1 and MD5 HMAC with RFC1321/2104/2403/2404 and FIPS180/FIPS198
- IPsec protocol processor
- High performance IPSEC Engine
- Random Number generator compliant with ANSI X9.31
- Public Key Crypto Engine supports high performance IKE and RSA computation
- Script Processor

CP4 capabilities

- FIPS-compliant DES/3DES/AES encryption and decryption
- SHA-1 and MD5 HMAC
- IPSEC protocol processor
- Random Number generator
- Public Key Crypto Engine
- Content processing engine
- ANSI X9.31 and PKCS#1 certificate support

Determining the content processor in your FortiGate unit

Use the `get hardware status` CLI command to determine which content processor your FortiGate unit contains. The output looks like this:

```
get hardware status
Model name: FortiGate-100D
ASIC version: CP8
ASIC SRAM: 64M
CPU: Intel(R) Atom(TM) CPU D525 @ 1.80GHz
Number of CPUs: 4
RAM: 1977 MB
Compact Flash: 15331 MB /dev/sda
Hard disk: 15272 MB /dev/sda
USB Flash: not available
Network Card chipset: Intel(R) PRO/1000 Network Connection (rev.0000)
Network Card chipset: bcm-sw Ethernet driver 1.0 (rev.)
```

The ASIC version line lists the content processor model number.

Viewing SSL acceleration status

You can view the status of SSL acceleration using the following command:

```
get vpn status ssl hw-acceleration-status
Acceleration hardware detected: kxp=on cipher=on
```

Disabling CP offloading for firewall policies

If you want to completely disable offloading to CP processors for test purposes or other reasons, you can do so in security policies. Here are some examples:

For IPv4 security policies.

```
config firewall policy
   edit 1
      set auto-asic-offload disable
   end
```

For IPv6 security policies.

```
config firewall policy6
   edit 1
      set auto-asic-offload disable
   end
```

For multicast security policies.

```
config firewall multicast-policy
   edit 1
      set auto-asic-offload disable
   end
```

Disabling `auto-asic-offload` also disables NP offloading.

Security processors (SPs)

FortiGate Security Processing (SP) modules, such as the SP3 but also including the XLP, XG2, XE2, FE8, and CE4, work at both the interface and system level to increase overall system performance by accelerating specialized security processing. You can configure the SP to favor IPS over firewall processing in hostile high-traffic environments.

SP processors include their own IPS engine which is similar to the FortiOS IPS engine but with the following limitations:

- The SP IPS engine does not support SSL deep inspection. When you have SSL deep inspection enabled for a security policy that includes flow-based inspection or IPS, offloading to the SP is disabled and traffic is processed by the FortiGate CPU and CP processors.
- The SP IPS engine does not support FortiGuard Web Filtering. When you enable flow-based FortiGuard Web Filtering on a FortiGate unit with an SP processor, the SP processor cannot perform FortiGuard lookups and web pages fail to load.

The following security processors are available:

- The SP3 (XLP) is built into the FortiGate-5101B and provides IPS acceleration. No special configuration is required. All IPS processing, including traffic accepted by IPv4 and IPv6 traffic policies and IPv4 and IPv6 DoS policies is accelerated by the built-in SP3 processors.
- The FMC-XG2 is an FMC module with two 10Gb/s SPF+ interfaces that can be used on FortiGate-3950B and FortiGate-3951B units.
- The FortiGate-3140B also contains a built-in XG2 using ports 19 and 20.

- The ADM-XE2 is a dual-width AMC module with two 10Gb/s interfaces that can be used on FortiGate-3810A and FortiGate-5001A-DW systems.
- The ADM-FE8 is a dual-width AMC module with eight 1Gb/s interfaces that can be used with the FortiGate-3810A.
- The ASM-CE4 is a single-width AMC module with four 10/100/1000 Mb/s interfaces that can be used on FortiGate-3016B and FortiGate-3810A units.

Traffic is blocked if you enable IPS for traffic passing over inter-VDOM links if that traffic is being offloaded by an SP processor.If you disable SP offloading traffic will be allowed to flow. You can disable offloading in individual firewall policies by disabling `auto-asic-offload` for individual policies. You can also use the following command to disable all IPS offloading

```
config ips global
   set np-accel-mode none
   set cp-accel-mode none
end
```

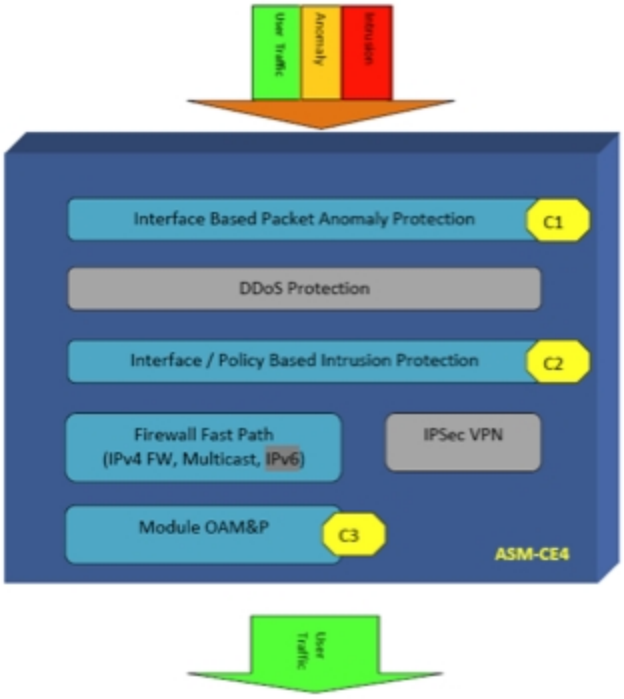
SP Processing Flow

SP processors provide an integrated high performance fast path multilayer solution for both intrusion protection and firewall functions. The multilayered protection starts from anomaly checking at packet level to ensure each packet is sound and reasonable. Immediately after that, a sophisticated set of interface based packet anomaly protection, DDoS protection, policy based intrusion protection, firewall fast path, and behavior based methods are employed to prevent DDoS attacks from the rest of system.

Then the packets enter an interface/policy based intrusion protection system,

where each packet is evaluated against a set of signatures. The end result is streams of user packets that are free of anomaly and attacks, entering the fast path system for unicast or multicast fast path forwarding.

SP processing flow



Displaying information about security processing modules

You can display information about installed SP modules using the CLI command

```
diagnose npu spm
```

For example, for the FortiGate-5101C:

```
FG-5101C # diagnose npu spm list
Available SP Modules:

ID Model      Slot     Interface
0 xh0         built-in  port1, port2, port3, port4,
                        base1, base2, fabric1, fabric2
                        eth10, eth11, eth12, eth13
                        eth14, eth15, eth16, eth17
                        eth18, eth19
```

You can also use this command to get more info about SP processing. This example shows how to display details about how the module is processing sessions using the syn proxy.

```
diagnose npu spm dos synproxy <sp_id>
```

This is a partial output of the command:

```
Number of proxied TCP connections :                 0
Number of working proxied TCP connections :         0
Number of retired TCP connections :                 0
Number of valid TCP connections :                   0
Number of attacks, no ACK from client :             0
Number of no SYN-ACK from server :                  0
Number of reset by server (service not supportted): 0
Number of estabilised session timeout :             0
```

```
Client timeout setting :                          3 Seconds
Server timeout setting :                          3 Seconds
```

Network processors (NP1, NP2, NP3, NP4 and NP6)

FortiASIC network processors work at the interface level to accelerate traffic by offloading traffic from the main CPU. Current models contain NP4 and NP6 network processors. Older FortiGate models include NP1 network processors (also known as FortiAccel, or FA2) and NP2 network processors.

The traffic that can be offloaded, maximum throughput, and number of network interfaces supported by each varies by processor model:

- NP6 supports offloading of most IPv4 and IPv6 traffic, IPsec VPN encryption, CAPWAP traffic, and multicast traffic. The NP6 has a capacity of 40 Gbps through 4 x 10 Gbps interfaces or 3 x 10 Gbps and 16 x 1 Gbps interfaces. For details about the NP6 processor, see NP6 Acceleration on page 1170 and for information about FortiGate models with NP6 processors, see FortiGate NP6 architectures on page 1185.
- NP4 supports offloading of most IPv4 firewall traffic and IPsec VPN encryption. The NP4 has a capacity of 20 Gbps through 2 x 10 Gbps interfaces. For details about NP4 processors, see NP4 Acceleration on page 1222 and for information about FortiGate models with NP4 processors, see FortiGate NP4 architectures on page 1237.
- NP2 supports IPv4 firewall and IPsec VPN acceleration. The NP2 has a capacity of 2 Gbps through 2 x 10 Gbps interfaces or 4 x 1 Gbps interfaces.
- NP1 supports IPv4 firewall and IPsec VPN acceleration with 2 Gbps capacity. The NP1 has a capacity of 2 Gbps through 2 x 1 Gbps interfaces.
  - The NP1 does not support frames greater than 1500 bytes. If your network uses jumbo frames, you may need to adjust the MTU (Maximum Transmission Unit) of devices connected to NP1 ports. Maximum frame size for NP2, NP4, and NP6 processors is 9216 bytes.
  - For both NP1 and NP2 network processors, ports attached to a network processor cannot be used for firmware installation by TFTP.

Sessions that require proxy-based and flow based security features (for example, virus scanning, IPS, application control and so on) are not fast pathed and must be processed by the CPU

Determining the network processors installed on your FortiGate unit

Use the following command to list the NP6 processors in your FortiGate unit:

```
diagnose npu np6 port-list
```

To list other network processors on your FortiGate unit, use the following CLI command.

```
get hardware npu <model> list
```

`<model>` can be `legacy`, `np1`, `np2` or `np4`.

The output lists the interfaces that have the specified processor. For example, for a FortiGate-5001B:

```
get hardware npu np4 list
ID    Model          Slot       Interface
0     On-board                  port1 port2 port3 port4
                                fabric1 base1 npu0-vlink0 npu0-vlink1
1     On-board                  port5 port6 port7 port8
                                fabric2 base2 npu1-vlink0 npu1-vlink1
```

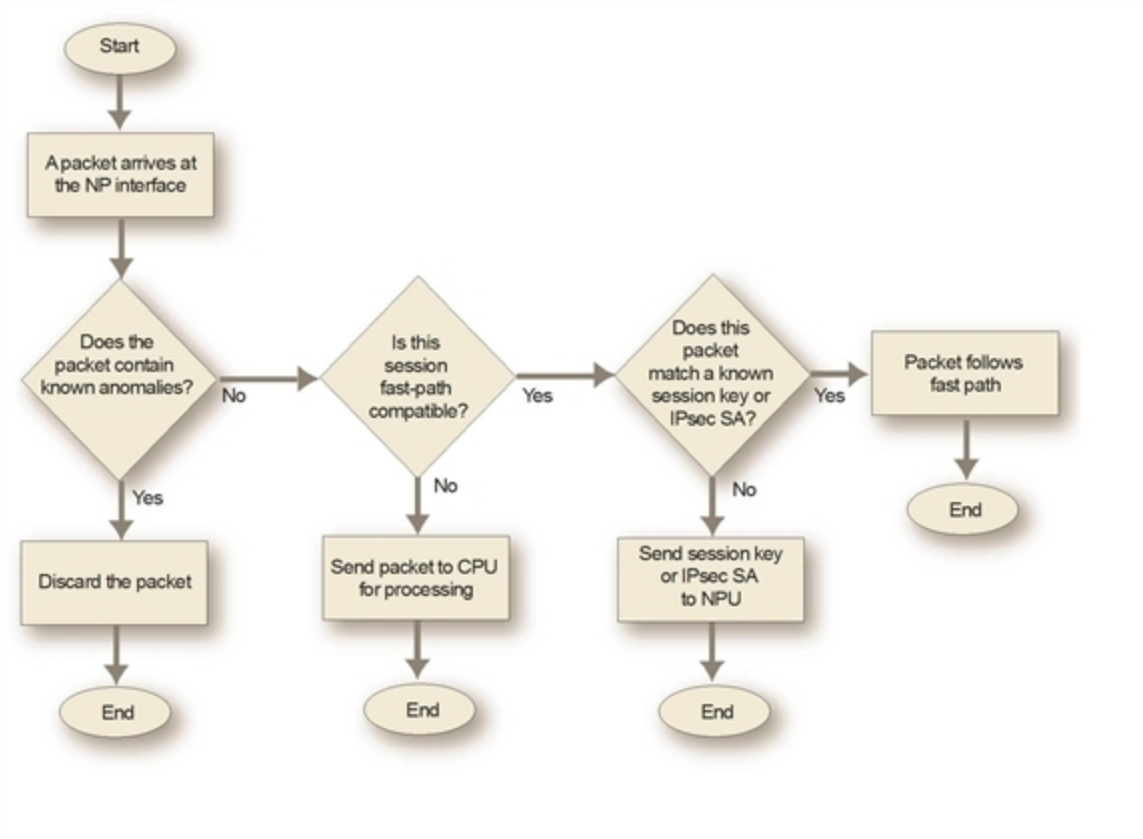
The `npu0-vlink0`, `npu1-vlink1` etc interfaces are used for accelerating inter-VDOM links.

How NP hardware acceleration alters packet flow

NP hardware acceleration generally alters packet flow as follows:

1. Packets initiating a session pass to the FortiGate unit's main processing resources (CPU).
2. The FortiGate unit assesses whether the session matches fast path (offload) requirements.
   To be suitable for offloading, traffic must possess only characteristics that can be processed by the fast path. The list of requirements depends on the processor, see NP6 session fast path requirements on page 1170 or NP4 session fast path requirements on page 1223.
   If the session can be fast pathed, the FortiGate unit sends the session key or IPsec security association (SA) and configured firewall processing action to the appropriate network processor.
3. Network processors continuously match packets arriving on their attached ports against the session keys and SAs they have received.
   - If a network processor's network interface is configured to perform hardware accelerated anomaly checks, the network processor drops or accepts packets that match the configured anomaly patterns. These checks are separate from and in advance of anomaly checks performed by IPS, which is not compatible with network processor offloading. See Offloading NP4 anomaly detection on page 1234.
   - The network processor next checks for a matching session key or SA. If a matching session key or SA is found, and if the packet meets packet requirements, the network processor processes the packet according to the configured action and then sends the resulting packet. This is the actual offloading step. Performing this processing on the NP processor improves overall performance because the NP processor is optimized for this task. As well, overall FortiGate performance is improved because the CPU has fewer sessions to process.

NP network processor packet flow



- If a matching session key or SA is not found, or if the packet does not meet packet requirements, the packet cannot be offloaded. The network processor sends the data to the FortiGate unit's CPU, which processes the packet.

Encryption and decryption of IPsec traffic originating from the FortiGate can utilize network processor encryption capabilities.

Packet forwarding rates vary by the percentage of offloadable processing and the type of network processing required by your configuration, but are independent of frame size. For optimal traffic types, network throughput can equal wire speed.

NP processors and traffic logging and monitoring

Except for the NP6, network processors do not count offloaded packets, and offloaded packets are not logged by traffic logging and are not included in traffic statistics and traffic log reports.

NP6 processors support per-session traffic and byte counters, Ethernet MIB matching, and reporting through messages resulting in traffic statistics and traffic log reporting.

Accelerated sessions on FortiView All Sessions page

When viewing sessions in the FortiView All Sessions console, NP4/ NP6 accelerated sessions are highlighted with an NP4 or NP6 icon. The tooltip for the icon includes the NP processor type and the total number of accelerated sessions.

You can also configure filtering to display FortiASIC sessions.

NP session offloading in HA active-active configuration

Network processors can improve network performance in active-active (load balancing) high availability (HA) configurations, even though traffic deviates from general offloading patterns, involving more than one network processor, each in a separate FortiGate unit. No additional offloading requirements apply.

Once the primary FortiGate unit's main processing resources send a session key to its network processor(s), network processor(s) on the primary unit can redirect any subsequent session traffic to other cluster members, reducing traffic redirection load on the primary unit's main processing resources.

As subordinate units receive redirected traffic, each network processor in the cluster assesses and processes session offloading independently from the primary unit. Session key states of each network processor are not part of synchronization traffic between HA members.

Configuring NP HMAC check offloading

Hash-based Message Authentication Code (HMAC) checks offloaded to network processors by default. You can enter the following command to disable this feature:

```
configure system global
   set ipsec-hmac-offload disable
end
```

Software switch interfaces and NP processors

FortiOS supports creating a software switch by grouping two or more FortiGate physical interfaces into a single virtual or software switch interface. All of the interfaces in this virtual switch act like interfaces in a hardware switch in that they all have the same IP address and can be connected to the same network. You create a software switch interface from the CLI using the command `config system switch-interface`.

The software switch is a bridge group of several interfaces, and the FortiGate CPU maintains the mac-port table for this bridge. As a result of this CPU involvement, traffic processed by a software switch interface is not offloaded to network processors.

Configuring NP accelerated IPsec VPN encryption/decryption offloading

Network processing unit (`npu`) settings configure offloading behavior for IPsec VPN. Configured behavior applies to all network processors in the FortiGate unit.

```
config system npu
   set enc-offload-antireplay {enable | disable}
   set dec-offload-antireplay {enable | disable}
   set offload-ipsec-host {enable | disable}
end
```

Variables	Description	Default
`enc-offload-antireplay {enable | disable}`	Enable or disable offloading of IPsec encryption. This option is used only when replay detection is enabled in Phase 2 configuration. If replay detection is disabled, encryption is always offloaded.	disable
`dec-offload-antireplay {enable | disable}`	Enable or disable offloading of IPsec decryption. This option is used only when replay detection is enabled in Phase 2 configuration. If replay detection is disabled, decryption is always offloaded.	enable
`offload-ipsec-host {enable | disable}`	Enable or disable offloading of IPsec encryption of traffic from local host (FortiGate unit). **Note:** For this option to take effect, the FortiGate unit must have previously sent the security association (SA) to the network processor.	disable

Example

You could configure the offloading of encryption and decryption for an IPsec SA that was sent to the network processor.

```
config system npu
   set enc-offload-antireplay enable
   set dec-offload-antireplay enable
   set offload-ipsec-host enable
end
```

Disabling NP acceleration for individual IPsec VPN phase 1s

Use the following command to disable NP offloading for an interface-based IPsec VPN phase 1:

```
config vpn ipsec phase1-interface
   edit phase-1-name
      set npu-offload disable
end
```

Use the following command to disable NP offloading for a policy-based IPsec VPN phase 1:

```
config vpn ipsec phase1
   edit phase-1-name
      set npu-offload disable
end
```

The `npu-offload` option is enabled by default.

Disabling NP offloading for unsupported IPsec encryption or authentication algorithms

In general, more recent IPsec VPN encryption and authentication algorithms may not be supported by older NP processors. For example, NP4 network processors do not support SHA-256, SHA-384, and SHA-512. IPsec traffic with unsupported algorithms is not offloaded and instead is processed by the FortiGate CPU. In addition, this configuration may cause packet loss and other performance issues. If you experience packet loss or performance

problems you should set the `npu-offload` option to `disable`. Future FortiOS versions should prevent selecting algorithms not supported by the hardware.

Disabling NP offloading for firewall policies

Use the following options to disable NP offloading for specific security policies:

For IPv4 security policies.

```
config firewall policy
   edit 1
      set auto-asic-offload disable
   end
```

For IPv6 security policies.

```
config firewall policy6
   edit 1
      set auto-asic-offload disable
   end
```

For multicast security policies.

```
config firewall multicast-policy
   edit 1
      set auto-asic-offload disable
   end
```

Enabling strict protocol header checking disables all hardware acceleration

You can use the following command to cause the FortiGate to apply strict header checking to verify that a packet is part of a session that should be processed. Strict header checking includes verifying the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options, and verifying that ESP packets have the correct sequence number, SPI, and data length.If the packet fails header checking it is dropped by the FortiGate unit.

```
config system global
   check-protocol-header strict
end.
```

Enabling strict header checking disables all hardware acceleration. This includes NP, SP.and CP processing.

sFlow and NetFlow and hardware acceleration

NP6 offloading is supported when you configure NetFlow for interfaces connected to NP6 processors.

Configuring sFlow on any interface disables all NP4 and NP6 offloading for all traffic on that interface. As well, configuring NetFlow on any interface disables NP4 offloading for all traffic on that interface.

Checking that traffic is offloaded by NP processors

A number of diagnose commands can be used to verify that traffic is being offloaded.

Using the packet sniffer

Use the packet sniffer to verify that traffic is offloaded. Offloaded traffic is not picked up by the packet sniffer so if you are sending traffic through the FortiGate unit and it is not showing up on the packet sniffer you can conclude that it is offloaded.

```
diag sniffer packet port1 <option>
```

Checking the firewall session offload tag

Use the `diagnose sys session list` command to display sessions. If the output for a session includes the `npu info` field you should see information about session being offloaded. If the output doesn't contain an `npu info` field then the session has not been offloaded.

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=34 expire=3565 timeout=3600
    flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=295/3/1 reply=60/1/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=48->6/6->48 gwy=10.1.100.11/11.11.11.1
hook=pre dir=org act=noop 172.16.200.55:56453->10.1.100.11:80(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.11:80->172.16.200.55:56453(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=4
serial=0000091c tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=172.16.200.55, bps=393
npu_state=00000000
npu info: flag=0x81/0x81, offload=4/4, ips_offload=0/0, epid=1/23, ipid=23/1,
    vlan=32779/0
```

Verifying IPsec VPN traffic offloading

The following commands can be used to verify IPsec VPN traffic offloading to NP processors.

```
diagnose vpn ipsec status
NP1/NP2/NP4_0/sp_0_0:
     null: 0 0
     des: 0 0
      3des: 4075 4074
     aes: 0 0
     aria: 0 0
     seed: 0 0
     null: 0 0
      md5: 4075 4074
     sha1: 0 0
     sha256: 0 0
     sha384: 0 0
     sha512: 0 0

diagnose vpn tunnel list
list all ipsec tunnel in vd 3
------------------------------------------------------
name=p1-vdom1 ver=1 serial=5 11.11.11.1:0->11.11.11.2:0 lgwy=static tun=tunnel
    mode=auto bound_if=47
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=3076 txp=1667 rxb=4299623276 txb=66323
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=20
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=p2-vdom1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
```

```
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=0000000e type=00 soft=0 mtu=1436 expire=1736 replaywin=2048 seqno=680
life: type=01 bytes=0/0 timeout=1748/1800
dec: spi=ae01010c esp=3des key=24 18e021bcace225347459189f292fbc2e4677563b07498a07
ah=md5 key=16 b4f44368741632b4e33e5f5b794253d3
enc: spi=ae01010d esp=3des key=24 42c94a8a2f72a44f9a3777f8e6aa3b24160b8af15f54a573
ah=md5 key=16 6214155f76b63a93345dcc9ec02d6415
dec:pkts/bytes=3073/4299621477, enc:pkts/bytes=1667/66375
 npu_flag=03 npu_rgwy=11.11.11.2 npu_lgwy=11.11.11.1 npu_selid=4

diagnose sys session list
session info: proto=6 proto_state=01 duration=34 expire=3565 timeout=3600
    flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/p1-vdom2
state=re may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=57->7/7->57 gwy=10.1.100.11/11.11.11.1
hook=pre dir=org act=noop 172.16.200.55:35254->10.1.100.11:80(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.11:80->172.16.200.55:35254(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=4
serial=00002d29 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=172.16.200.55, bps=260
npu_state=00000000
npu info: flag=0x81/0x82, offload=7/7, ips_offload=0/0, epid=1/3, ipid=3/1,
    vlan=32779/0
```

Controlling IPS NPx and CPx acceleration

You can use the following commands to enable or disable acceleration of IPS processing by NPx and CPx processors:

```
config ips global
   set np-accel-mode {none | basic}
   set cp-accel-mode {none | basic | advanced}
end
```

The network processor (NP) acceleration modes are:

`none`: Network Processor acceleration disabled

`basic`: Basic Network Processor acceleration enabled (currently the same as `basic` but will be enhanced in a future FortiOS release).

The content processor (CP) acceleration modes are:

`none`: Content Processor acceleration disabled

`basic`: Basic Content Processor acceleration enabled

`advanced`: Advanced Content Processor acceleration enabled

Dedicated Management CPU

The web-based manager and CLI of FortiGate units with NP6 and NP4 processors may become unresponsive when the system is under heavy processing load because NP6 or NP4 interrupts overload the CPUs preventing CPU cycles from being used for management tasks. You can resolve this issue by using the following command to dedicate CPU core 0 to management tasks.

```
config system npu
   set dedicated-management-cpu {enable | disable}
end
```

All management tasks are then processed by CPU 0 and NP6 or NP4 interrupts are handled by the remaining CPU cores.

Offloading flow-based content inspection with NTurbo and IPSA

You can use the following command to configure NTurbo and IPSA offloading and acceleration of firewall sessions that include flow-based security profiles to NPx and CPx processors. NTurbo and IPSA can offload firewall sessions that include IPS, application control, CASI, flow-based antivirus, and flow-based web filtering security profiles.

```
config ips global
   set np-accel-mode {none | basic}
   set cp-accel-mode {none | basic | advanced}
end
```

NTurbo offloads firewall sessions with flow-based security profiles to NPx processors

NTurbo offloads firewall sessions that include flow-based security profiles to NP4 or NP6 network processors. Without NTurbo, or with NTurbo disabled, all firewall sessions that include flow-based security profiles are processed by the FortiGate CPU.

NTurbo can only offload firewall sessions containing flow-based security profiles if the session could otherwise have been offloaded except for the presence of the flow-based security profiles. If something else prevents the session from being offloaded, NTurbo will not offload that session.

Firewall sessions that include proxy-based security profiles are never offloaded to network processors and are always processed by the FortiGate CPU.

NTurbo creates a special data path to redirect traffic from the ingress interface to IPS, and from IPS to the egress interface. NTurbo allows firewall operations to be offloaded along this path, and still allows IPS to behave as a stage in the processing pipeline, reducing the workload on the FortiGate CPU and improving overall throughput.

NTurbo sessions still offload pattern matching and other processes to CP processors, just like normal flow-based sessions.

If NTurbo is supported by your FortiGate unit, you can use the following command to configure it:

```
config ips global
```

```
    set np-accel-mode {basic | none}
end
```

`basic` enables NTurbo and is the default setting for FortiGate models that support NTurbo. `none` disables NTurbo. If the `np-accel-mode` option is not available, then your FortiGate does not support NTurbo.

There are some special cases where sessions may not be offloaded by NTurbo, even when NTurbo is explicitly enabled. In these cases the sessions are handled by the FortiGate CPU.

- NP acceleration is disabled. For example, `auto-asic-offload` is disabled in the firewall policy configuration.
- The firewall policy includes proxy-based security profiles.
- The sessions require FortiOS session-helpers. For example, FTP sessions can not be offloaded to NP processors because FTP sessions use the FTP session helper.
- Interface policies or DoS policies have been added to the ingress or egress interface.
- Tunneling is enabled. Any traffic to or from a tunnelled interface (IPSec, IPinIP, SSL VPN, GRE, CAPWAP etc.) cannot be offloaded by NTurbo.

IPSA offloads flow-based enhanced pattern matching to CPx processors

IPSA offloads enhanced pattern matching operations required for flow-based content processing to Content Processors (CPs) such as the CP7, CP8 and CP9. IPSA offloads enhanced pattern matching for NTurbo firewall sessions and firewall sessions that are not offloaded to NP processors. When IPSA is turned on, flow-based pattern databases are compiled and downloaded to the content processors. Flow-based pattern matching requests are redirected to the CP hardware reducing the load on the FortiGate CPU. In addition the CP processors accelerate pattern matching.

IF IPSA is supported on your FortiGate unit, you can use the following command to configure it:

```
config ips global
   set cp-accel-mode {advanced | basic | none}
end
```

`basic` offloads basic pattern matching. `advanced` offloads more types of pattern matching resulting in higher throughput than basic mode. `advanced` is only available on FortiGate models with two or more CP8 processors or one or more CP9 processors. If the `cp-accel-mode` option is not available, then your FortiGate does not support IPSA.

On FortiGates with one CP7 or CP8 processor the default `cp-accel-mode` is `basic`.Setting the mode to `advanced` does not change the types of pattern matching that are offloaded.

On FortiGates with two or more CP8 processors or one or more CP9 processors the default `cp-accel-mode` is `advanced`. You can set the mode to `basic` to offload fewer types of pattern matching.

NP6 Acceleration

NP6 network processors provide fastpath acceleration by offloading communication sessions from the FortiGate CPU. When the first packet of a new session is received by an interface connected to an NP6 processor, just like any session connecting with any FortiGate interface, the session is forwarded to the FortiGate CPU where it is matched with a security policy. If the session is accepted by a security policy and if the session can be offloaded its session key is copied to the NP6 processor that received the packet. All of the rest of the packets in the session are intercepted by the NP6 processor and fast-pathed out of the FortiGate unit to their destination without ever passing through the FortiGate CPU. The result is enhanced network performance provided by the NP6 processor plus the network processing load is removed from the CPU. In addition the NP6 processor can handle some CPU intensive tasks, like IPsec VPN encryption/decryption.

Session keys (and IPsec SA keys) are stored in the memory of the NP6 processor that is connected to the interface that received the packet that started the session. All sessions are fast-pathed and accelerated, even if they exit the FortiGate unit through an interface connected to another NP6. There is no dependence on getting the right pair of interfaces since the offloading is done by the receiving NP6.

The key to making this possible is an Integrated Switch Fabric (ISF) that connects the NP6s and the FortiGate unit interfaces together. Many FortiGate units with NP6 processors also have an ISF. The ISF allows any port connectivity. All ports and NP6s can communicate with each other over the ISF. There are no special ingress and egress fast path requirements as long as traffic enters and exits on interfaces connected to the same ISF.

Some FortiGate units, such as the FortiGate-1000D include multiple NP6 processors that are not connected by an ISF. Because the ISF is not present fast path acceleration is supported only between interfaces connected to the same NP6 processor. Since the ISF introduces some latency, models with no ISF provide low-latency network acceleration between network interfaces connected to the same NP6 processor.

There are at least two limitations to keep in mind:

- The capacity of each NP6 processor. An individual NP6 processor can support between 10 and 16 million sessions. This number is limited by the amount of memory the processor has. Once an NP6 processor hits its session limit, sessions that are over the limit are sent to the CPU. You can avoid this problem by as much as possible distributing incoming sessions evenly among the NP6 processors. To be able to do this you need to be aware of which interfaces connect to which NP6 processors and distribute incoming traffic accordingly.
- Some FortiGate units may use some NP6 processors for special functions. For example, ports 25 to 32 of the FortiGate-3700D can be used for low latency offloading.

NP6 session fast path requirements

NP6 processors can offload the following traffic and services:

- IPv4 and IPv6 traffic and NAT64 and NAT46 traffic (as well as IPv4 and IPv6 versions of the following traffic types where appropriate)
- Link aggregation (LAG) (IEEE 802.3ad) traffic (see Increasing NP6 offloading capacity using link aggregation groups (LAGs) on page 1175)
- TCP, UDP, ICMP and SCTP traffic
- IPsec VPN traffic, and offloading of IPsec encryption/decryption (including SHA2-256 and SHA2-512)
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- SIT and IPv6 Tunnelling sessions

- Multicast traffic (including Multicast over IPsec)
- CAPWAP and wireless bridge traffic tunnel encapsulation to enable line rate wireless forwarding from FortiAP devices
- Traffic shaping and priority queuing for both shared and per IP traffic shaping.
- Syn proxying
- Inter-VDOM link traffic

Sessions that are offloaded must be fast path ready. For a session to be fast path ready it must meet the following criteria:

- Layer 2 type/length must be 0x0800 for IPv4 or 0x86dd for IPv6 (IEEE 802.1q VLAN specification is supported)
- Layer 3 protocol can be IPv4 or IPv6
- Layer 4 protocol can be UDP, TCP, ICMP, or SCTP
- In most cases, Layer 3 / Layer 4 header or content modification sessions that require a session helper can be offloaded.
- Local host traffic (originated by the FortiGate unit) can be offloaded
- If the FortiGate supports, NTurbo sessions can be offloaded if they are accepted by firewall policies that include IPS, Application Control, flow-based antivirus, or flow-based web filtering.

Offloading Application layer content modification is not supported. This means that sessions are not offloaded if they are accepted by firewall policies that include proxy-based virus scanning, proxy-based web filtering, DNS filtering, DLP, email filtering, VoIP, ICAP, or Proxy options.

If you disable anomaly checks by Intrusion Prevention (IPS), you can still enable hardware accelerated anomaly checks using the `fp-anomaly` field of the `config system interface` CLI command. See Configuring individual NP6 processors on page 1178.

If a session or is not fast path ready, the FortiGate unit will not send the session key or IPsec SA key to the NP6 processor. Without the session key, all session key lookup by a network processor for incoming packets of that session fails, causing all session packets to be sent to the FortiGate unit's main processing resources, and processed at normal speeds.

If a session is fast path ready, the FortiGate unit will send the session key or IPsec SA key to the network processor. Session key or IPsec SA key lookups then succeed for subsequent packets from the known session or IPsec SA.

Packet fast path requirements

Packets within the session must then also meet packet requirements.

- Incoming packets must not be fragmented.
- Outgoing packets must not require fragmentation to a size less than 385 bytes. Because of this requirement, the configured MTU (Maximum Transmission Unit) for a network processor's network interfaces must also meet or exceed the network processors' supported minimum MTU of 385 bytes.

Mixing fast path and non-fast path traffic

If packet requirements are not met, an individual packet will be processed by the FortiGate CPU regardless of whether other packets in the session are offloaded to the NP6.

Also, in some cases, a protocol's session(s) may receive a mixture of offloaded and non-offloaded processing. For example, VoIP control packets may not be offloaded but VoIP data packets (voice packets) may be offloaded.

NP6 processors and traffic shaping

NP6-offloaded traffic supports traffic shaping just like any other traffic with one exception: configuring in bandwith traffic shaping has no effect on NP6 accelerated traffic. In bandwidth traffic shaping sets the bandwidth limit for incoming traffic for an interface.

Out bandwidth traffic shaping is supported. Out bandwidth traffic shaping sets the bandwidth limit for outgoing traffic for an interface. You can use the following command to configure out bandwidth traffic shaping:

```
config system interface
   edit port1
      set outbandwidth 2000
   end
```

Viewing your FortiGate NP6 processor configuration

Use the following command to view the NP6 processor configuration of your FortiGate unit:

```
diagnose npu np6 port-list
```

For example output of this command for different FortiGate models, see FortiGate NP6 architectures on page 1185.

Use either of the following commands to view the NP6 processor hardware configuration of your FortiGate unit:

```
get hardware npu np6 port-list
diagnose npu np6 port-list
```

For example, for the FortiGate-5001D the output would be:

```
get hardware npu np6 port-list
Chip   XAUI Ports            Max   Cross-chip
                             Speed offloading
------ ---- -------          ----- ----------
np6_0  0    port3            10G   Yes
       1
       2    base1            1G    Yes
       3
       0-3  port1            40G   Yes
       0-3  fabric1          40G   Yes
       0-3  fabric3          40G   Yes
       0-3  fabric5          40G   Yes
------ ---- -------          ----- ----------
np6_1  0
       1    port4            10G   Yes
       2
       3    base2            1G    Yes
       0-3  port2            40G   Yes
       0-3  fabric2          40G   Yes
       0-3  fabric4          40G   Yes
------ ---- -------          ----- ----------
```

For more example output for different FortiGate models, see FortiGate NP6 architectures on page 1.

You can also use the following command to view the offloading features enabled or disabled on each of the NP6 processors in your FortiGate unit:

```
diagnose npu np6 npu-feature
                    np_0      np_1
------------------- --------- ---------
Fastpath            Enabled   Enabled
Low-latency-mode    Disabled  Disabled
Low-latency-cap     No        No
IPv4 firewall       Yes       Yes
IPv6 firewall       Yes       Yes
IPv4 IPSec          Yes       Yes
IPv6 IPSec          Yes       Yes
IPv4 tunnel         Yes       Yes
IPv6 tunnel         Yes       Yes
GRE tunnel          No        No
IPv4 Multicast      Yes       Yes
IPv6 Multicast      Yes       Yes
CAPWAP              Yes       Yes
```

Optimizing NP6 performance by distributing traffic to XAUI links

On most FortiGate units with NP6 processors, the FortiGate interfaces are switch ports that connect to the NP6 processors with XAUI links. Packets pass from the interfaces to the NP6 processor over the XAUI links. Each NP6 processor has a 40 Gigabit bandwidth capacity. The four XAUI links each have a 10 Gigabit capacity for a total of 40 Gigabits.

On many FortiGate units with NP6 processors, the NP6 processors and the XAUI links are over-subscribed. Since the NP6 processors are connected by an Integrated Switch Fabric, you do not have control over how traffic is distributed to them. In fact traffic is distributed evenly by the ISF.

However, you can control how traffic is distributed to the XAUI links and you can optimize performance by distributing traffic evenly among the XAUI links. For example, if you have a very high amount of traffic passing between two networks, you can connect each network to interfaces connected to different XAUI links to distribute the traffic for each network to a different XAUI link.

For example, on a FortiGate-3200D (See Optimizing NP6 performance by distributing traffic to XAUI links), there are 48 10-Gigabit interfaces that send and receive traffic for two NP6 processors over a total of eight 10-Gigabit XAUI links. Each XAUI link gets traffic from six 10-Gigabit FortiGate interfaces. The amount of traffic that the FortiGate-3200D can offload is limited by the number of NP6 processors and the number of XAUI links. You can optimize the amount of traffc that the FortiGate-3200D can process by distributing it evenly amount the XAUI links and the NP6 processors.

You can see the Etherent interface, XAUI link, and NP6 configuration by entering the `get hardware npu np6 port-list` command. For the FortiGate-3200D the output is:

```
get hardware npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0    port1   10G   Yes
       0    port5   10G   Yes
       0    port10  10G   Yes
       0    port13  10G   Yes
```

```
        0    port17  10G   Yes
        0    port22  10G   Yes
        1    port2   10G   Yes
        1    port6   10G   Yes
        1    port9   10G   Yes
        1    port14  10G   Yes
        1    port18  10G   Yes
        1    port21  10G   Yes
        2    port3   10G   Yes
        2    port7   10G   Yes
        2    port12  10G   Yes
        2    port15  10G   Yes
        2    port19  10G   Yes
        2    port24  10G   Yes
        3    port4   10G   Yes
        3    port8   10G   Yes
        3    port11  10G   Yes
        3    port16  10G   Yes
        3    port20  10G   Yes
        3    port23  10G   Yes
------ ---- ------- ----- ----------
np6_1   0    port26  10G   Yes
        0    port29  10G   Yes
        0    port33  10G   Yes
        0    port37  10G   Yes
        0    port41  10G   Yes
        0    port45  10G   Yes
        1    port25  10G   Yes
        1    port30  10G   Yes
        1    port34  10G   Yes
        1    port38  10G   Yes
        1    port42  10G   Yes
        1    port46  10G   Yes
        2    port28  10G   Yes
        2    port31  10G   Yes
        2    port35  10G   Yes
        2    port39  10G   Yes
        2    port43  10G   Yes
        2    port47  10G   Yes
        3    port27  10G   Yes
        3    port32  10G   Yes
        3    port36  10G   Yes
        3    port40  10G   Yes
        3    port44  10G   Yes
        3    port48  10G   Yes
------ ---- ------- ----- ----------
```

In this command output you can see that each NP6 has for four XAUI links (0 to 3) and that each XAUI link is connected to six 10-gigabit Ethernet interfaces. To optimize throughput you should keep the amount of traffic being processed by each XAUI port to under 10 Gbps. So for example, if you want to offload traffic from four 10-gigabit networks you can connect these networks to Ethernet interfaces 1, 2, 3 and 4. This distributes the traffic from each 10-Gigabit network to a different XAUI link. Also, if you wanted to offload traffic from four more 10-

Gigabit networks you could connect them to Ethernet ports 26, 25, 28, and 27. As a result each 10-Gigabit network would be connected to a different XAUI link.

Increasing NP6 offloading capacity using link aggregation groups (LAGs)

NP6 processors can offload sessions received by interfaces in link aggregation groups (LAGs) (IEEE 802.3ad). A 802.3ad Link Aggregation and it's management protocol, Link Aggregation Control Protocol (LACP) LAG combines more than one physical interface into a group that functions like a single interface with a higher capacity than a single physical interface. For example, you could use a LAG if you want to offload sessions on a 30 Gbps link by adding three 10-Gbps interfaces to the same LAG.

All offloaded traffic types are supported by LAGs, including IPsec VPN traffic. Just like with normal interfaces, traffic accepted by a LAG is offloaded by the NP6 processor connected to the interfaces in the LAG that receive the traffic to be offloaded. If all interfaces in a LAG are connected to the same NP6 processor, traffic received by that LAG is offloaded by that NP6 processor. The amount of traffic that can be offloaded is limited by the capacity of the NP6 processor.

If a FortiGate has two or more NP6 processors connected by an integrated switch fabric (ISF), you can use LAGs to increase offloading by sharing the traffic load across multiple NP6 processors. You do this by adding physical interfaces connected to different NP6 processors to the same LAG.

Adding a second NP6 processor to a LAG effectively doubles the offloading capacity of the LAG. Adding a third further increases offloading. The actual increase in offloading capacity may not actually be doubled by adding a second NP6 or tripled by adding a thrid. Traffic and load conditions and other factors may limit the actual offloading result.

The increase in offloading capacity offered by LAGs and multiple NP6s is supported by the integrated switch fabric (ISF) that allows multiple NP6 processors to share session information. Most FortiGate units with multiple NP6 processors also have an ISF. However, the FortiGate-1000D does not have an ISF. On this model and others that have more than one NP6 and no ISF, if you attempt to add interfaces connected to different NP6 processors to a LAG the system displays an error message.

There are also a few limitations to LAG NP6 offloading support for IPsec VPN:

- IPsec VPN anti-replay protection cannot be used if IPSec is configured on a LAG that has interfaces connected to multiple NP6 processors.
- Because the encrypted traffic for one IPsec VPN tunnel has the same 5-tuple, the traffic from one tunnel can only can be balanced to one interface in a LAG. This limits the maximum throughput for one IPsec VPN tunnel in an NP6 LAG group to 10Gbps.

Configuring Inter-VDOM link acceleration with NP6 processors

FortiGate units with NP6 processors include inter-VDOM links that can be used to accelerate inter-VDOM link traffic.

- For a FortiGate unit with two NP6 processors there are two accelerated inter-VDOM links, each with two interfaces:
  - **npu0_vlink:**
    npu0_vlink0
    npu0_vlink1
  - **npu1_vlink:**
    npu1_vlink0
    npu1_vlink1

These interfaces are visible from the GUI and CLI. For a FortiGate unit with NP6 interfaces, enter the following CLI command to display the NP6-accelerated inter-VDOM links:

```
get system interface
...
== [ npu0_vlink0 ]
name: npu0_vlink0 mode: static ip: 0.0.0.0 0.0.0.0 status: down netbios-forward: disable
    type: physical sflow-sampler: disable explicit-web-proxy: disable explicit-ftp-proxy:
    disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-
    fragment: disable

== [ npu0_vlink1 ]
name: npu0_vlink1 mode: static ip: 0.0.0.0 0.0.0.0 status: down netbios-forward: disable
    type: physical sflow-sampler: disable explicit-web-proxy: disable explicit-ftp-proxy:
    disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-
    fragment: disable

== [ npu1_vlink0 ]
name: npu1_vlink0 mode: static ip: 0.0.0.0 0.0.0.0 status: down netbios-forward: disable
    type: physical sflow-sampler: disable explicit-web-proxy: disable explicit-ftp-proxy:
    disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-
    fragment: disable

== [ npu1_vlink1 ]
name: npu1_vlink1 mode: static ip: 0.0.0.0 0.0.0.0 status: down netbios-forward: disable
    type: physical sflow-sampler: disable explicit-web-proxy: disable explicit-ftp-proxy:
    disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-
    fragment: disable
...
```

By default the interfaces in each inter-VDOM link are assigned to the root VDOM. To use these interfaces to accelerate inter-VDOM link traffic, assign each interface in the pair to the VDOMs that you want to offload traffic between. For example, if you have added a VDOM named New-VDOM to a FortiGate unit with NP4 processors, you can go to **System > Network > Interfaces** and edit the **npu0-vlink1** interface and set the **Virtual Domain** to **New-VDOM**. This results in an accelerated inter-VDOM link between root and New-VDOM. You can also do this from the CLI:

```
config system interface
   edit npu0-vlink1
      set vdom New-VDOM
end
```

Using VLANs to add more accelerated Inter-VDOM links

You can add VLAN interfaces to the accelerated inter-VDOM links to create inter-VDOM links between more VDOMs. For the links to work, the VLAN interfaces must be added to the same inter-VDOM link, must be on the same subnet, and must have the same VLAN ID.

For example, to accelerate inter-VDOM link traffic between VDOMs named Marketing and Engineering using VLANs with VLAN ID 100 go to **System > Network > Interfaces** and select **Create New** to create the VLAN interface associated with the Marketing VDOM:

Name	Marketing-link
Type	VLAN
Interface	npu0_vlink0
VLAN ID	100
Virtual Domain	Marketing
IP/Network Mask	172.20.120.12/24

Create the inter-VDOM link associated with Engineering VDOM:

Name	Engineering-link
Type	VLAN
Interface	npu0_vlink1
VLAN ID	100
Virtual Domain	Engineering
IP/Network Mask	172.20.120.22/24

Or do the same from the CLI:

```
config system interface
   edit Marketing-link
      set vdom Marketing
      set ip 172.20.120.12/24
      set interface npu0_vlink0
      set vlanid 100
   next
   edit Engineering-link
      set vdom Engineering
      set ip 172.20.120.22/24
      set interface npu0_vlink1
      set vlanid 100
```

Confirm that the traffic is accelerated

Use the following CLI commands to obtain the interface index and then correlate them with the session entries. In the following example traffic was flowing between new accelerated inter-VDOM links and physical ports port1 and port 2 also attached to the NP6 processor.

```
diagnose ip address list
IP=172.31.17.76->172.31.17.76/255.255.252.0 index=5 devname=port1
IP=10.74.1.76->10.74.1.76/255.255.252.0 index=6 devname=port2
IP=172.20.120.12->172.20.120.12/255.255.255.0 index=55 devname=IVL-VLAN1_ROOT
IP=172.20.120.22->172.20.120.22/255.255.255.0 index=56 devname=IVL-VLAN1_VDOM1
```

```
diagnose sys session list
session info: proto=1 proto_state=00 duration=282 expire=24 timeout=0 session info:
    proto=1 proto_state=00 duration=124 expire=59 timeout=0 flags=00000000
    sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=180/3/1 reply=120/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=55->5/5->55
    gwy=172.31.19.254/172.20.120.22
hook=post dir=org act=snat 10.74.2.87:768->10.2.2.2:8(172.31.17.76:62464)
hook=pre dir=reply act=dnat 10.2.2.2:62464->172.31.17.76:0(10.74.2.87:768)
misc=0 policy_id=4 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=0000004e tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=10.74.2.87, bps=880
npu_state=00000000
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=160/218, ipid=218/160,
    vlan=32769/0


session info: proto=1 proto_state=00 duration=124 expire=20 timeout=0 flags=00000000
    sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=180/3/1 reply=120/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=6->56/56->6
    gwy=172.20.120.12/10.74.2.87
hook=pre dir=org act=noop 10.74.2.87:768->10.2.2.2:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.2.2.2:768->10.74.2.87:0(0.0.0.0:0)
misc=0 policy_id=3 id_policy_id=0 auth_info=0 chk_client_info=0 vd=1
serial=0000004d tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=10.74.2.87, bps=880
npu_state=00000000
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=219/161, ipid=161/219,
    vlan=0/32769
total session 2
```

Configuring individual NP6 processors

You can use the `config system np6` command to configure a wide range of settings for the NP6 processors in your FortiGate unit including enabling/disabling fastpath and low latency and adjusting session timeouts. As well you can set anomaly checking for IPv4 and IPv6 traffic. You can also configure different settings for each NP6 processor.

The settings that you configure for an NP6 processor with the `config system np6` command apply to traffic processed by all interfaces connected to the NP6 processor. This includes the physical interfaces connected to the NP6 processor as well as all subinterfaces, VLAN interfaces, IPsec interfaces, LAGs and so on associated with the physical interfaces connected to the NP6 processor.

Some of the options for this command apply anomaly checking for NP6 sessions in the same way as the command described in Offloading NP4 anomaly detection on page 1234 applies anomaly checking for for NP4 sessions.

```
config system np6
   edit <np6-processor-name>
      set fastpath {disable | enable}
      set low-latency-mode {disable | enable}
      set per-session-accounting {disable | enable}
      set session-timeout-random-range <range>
      set garbage-session-collector {disable | enable}
      set session-collector-interval <range>
      set session-timeout-interval <range>
      set session-timeout-random-range <range>
      set session-timeout-fixed {disable | enable}
         config fp-anomaly-v4
            set icmp-frag {allow | drop | trap-to-host}
            set icmp-land {allow | drop | trap-to-host}
            set ipv4-land {allow | drop | trap-to-host}
            set ipv4-optlsrr {allow | drop | trap-to-host}
            set ipv4-optrr {allow | drop | trap-to-host}
            set ipv4-optsecurity {allow | drop | trap-to-host}
            set ipv4-optssrr {allow | drop | trap-to-host}
            set ipv4-optstream {allow | drop | trap-to-host}
            set ipv4-opttimestamp {allow | drop | trap-to-host}
            set ipv4-proto-err {allow | drop | trap-to-host}
            set ipv4-unknopt {allow | drop | trap-to-host}
            set tcp-land {allow | drop | trap-to-host}
            set tcp-syn-fin {allow | drop | trap-to-host}
            set tcp-winnuke {allow | drop | trap-to-host}
            set tcp_fin_noack {allow | drop | trap-to-host}
            set tcp_fin_only {allow | drop | trap-to-host}
            set tcp_no_flag {allow | drop | trap-to-host}
            set tcp_syn_data {allow | drop | trap-to-host}
            set udp-land {allow | drop | trap-to-host}
         end
         config fp-anomaly-v6
            set ipv6-daddr_err {allow | drop | trap-to-host}
            set ipv6-land {allow | drop | trap-to-host}
            set ipv6-optendpid {allow | drop | trap-to-host}
            set ipv6-opthomeaddr {allow | drop | trap-to-host}
            set ipv6-optinvld {allow | drop | trap-to-host}
            set ipv6-optjumbo {allow | drop | trap-to-host}
            set ipv6-optnsap {allow | drop | trap-to-host}
            set ipv6-optralert {allow | drop | trap-to-host}
            set ipv6-opttunnel {allow | drop | trap-to-host}
            set ipv6-proto-err {allow | drop | trap-to-host}
            set ipv6-saddr_err {allow | drop | trap-to-host}
            set ipv6-unknopt {allow | drop | trap-to-host}
         end
```

Command syntax

Command	Description	Default
`fastpath {disable | enable}`	Enable fastpath acceleration to offload sessions to the NP6 processor. You can disable fastpath if you don't want the NP6 processor to offload sessions.	enable
`low-latency-mode {disable | enable}`	Enable low-latency mode. In low latency mode the integrated switch fabric is bypassed. Low latency mode requires that packet enter and exit using the same NP6 processor. This option is only available for NP6 processors that can operate in low-latency mode.	disable
`per-session-accounting {disable | enable}`	Record traffic log messages for offloaded sessions. Enabling this feature reduces performance..	disable
`garbage-session-collector {disable | enable}`	Enable deleting expired or garbage sessions.	disable
`session-collector-interval <range>`	Set the expired or garbage session collector time interval in seconds. The range is 1 to 100 seconds.	8
`session-timeout-interval <range>`	Set the timeout for inactive sessions. The range is 0 to 1000 seconds.	40
`session-timeout-random-range <range>`	Set the random timeout for inactive sessions. The range is 0 to 1000 seconds.	8
`session-timeout-fixed {disable | enable}`	Force session timeouts at fixed instead of random intervals.	disable
config fp-anomaly-v4		
`fp-anomaly-v4`	Configure how the NP6 processor does IPv4 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called "trap-to-host"). Selecting "trap-to-host" turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy.	
`icmp-frag {allow | drop | trap-to-host}`	Detects Layer 3 fragmented packets that could be part of a layer 4 ICMP anomalies.	allow
`icmp-land {allow | drop | trap-to-host}`	Detects ICMP land anomalies.	trap-to-host
`ipv4-land {allow | drop | trap-to-host}`	Detects IPv4 land anomalies.	trap-to-host

Command	Description	Default
`ipv4-optlsrr {allow | drop | trap-to-host}`	Detects IPv4 with loose source record route option anomalies.	trap-to-host
`ipv4-optrr {allow | drop | trap-to-host}`	Detects IPv4 with record route option anomalies.	trap-to-host
`ipv4-optsecurity {allow | drop | trap-to-host}`	Detects security option anomalies.	trap-to-host
`ipv4-optssrr {allow | drop | trap-to-host}`	Detects IPv4 with strict source record route option anomalies.	trap-to-host
`ipv4-optstream {allow | drop | trap-to-host}`	Detects stream option anomalies.	trap-to-host
`ipv4-opttimestamp {allow | drop | trap-to-host}`	Detects timestamp option anomalies.	trap-to-host
`ipv4-proto-err {allow | drop | trap-to-host}`	Detects invalid layer 4 protocol anomalies.	trap-to-host
`ipv4-unknopt {allow | drop | trap-to-host}`	Detects unknown option anomalies.	trap-to-host
`tcp-land {allow | drop | trap-to-host}`	Detects TCP land anomalies.	trap-to-host
`tcp-syn-fin {allow | drop | trap-to-host}`	Detects TCP SYN flood SYN/FIN flag set anomalies.	allow
`tcp-winnuke {allow | drop | trap-to-host}`	Detects TCP WinNuke anomalies.	trap-to-host
`tcp_fin_noack {allow | drop | trap-to-host}`	Detects TCP SYN flood with FIN flag set without ACK setting anomalies.	trap-to-host
`tcp_fin_only {allow | drop | trap-to-host}`	Detects TCP SYN flood with only FIN flag set anomalies.	trap-to-host
`tcp_no_flag {allow | drop | trap-to-host}`	Detects TCP SYN flood with no flag set anomalies.	allow
`tcp_syn_data {allow | drop | trap-to-host}`	Detects TCP SYN flood packets with data anomalies.	allow
`udp-land {allow | drop | trap-to-host}`	Detects UDP land anomalies.	trap-to-host

Command	Description	Default
config fp-anomaly-v6		
`fp-anomaly-v6`	Configure how the NP6 processor does IPv6 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called “trap-to-host”). Selecting “trap-to-host” turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy.	
`ipv6-daddr_err {allow | drop | trap-to-host}`	Detects destination address as unspecified or loopback address anomalies.	trap-to-host
`ipv6-land {allow | drop | trap-to-host}`	Detects IPv6 land anomalies	trap-to-host
`ipv6-optendpid {allow | drop | trap-to-host}`	Detects end point identification anomalies.	trap-to-host
`ipv6-opthomeaddr {allow | drop | trap-to-host}`	Detects home address option anomalies.	trap-to-host
`ipv6-optinvld {allow | drop | trap-to-host}`	Detects invalid option anomalies.	trap-to-host
`ipv6-optjumbo {allow | drop | trap-to-host}`	Detects jumbo options anomalies.	trap-to-host
`ipv6-optnsap {allow | drop | trap-to-host}`	Detects network service access point address option anomalies.	trap-to-host
`ipv6-optralert {allow | drop | trap-to-host}`	Detects router alert option anomalies.	trap-to-host
`ipv6-opttunnel {allow | drop | trap-to-host}`	Detects tunnel encapsulation limit option anomalies.	trap-to-host
`ipv6-proto-err {allow | drop | trap-to-host}`	Detects layer 4 invalid protocol anomalies.	trap-to-host
`ipv6-saddr_err {allow | drop | trap-to-host}`	Detects source address as multicast anomalies.	trap-to-host
`ipv6-unknopt {allow | drop | trap-to-host}`	Detects unknown option anomalies.	trap-to-host

Enabling per-session accounting for offloaded NP6 sessions

By default FortiOS does not record log messages for offloaded NP6 and NP4 sessions. This also means that traffic monitoring does not report correct session counts, byte counts and packet counts for offloaded NP6 and NP4 sessions.

However, for NP6 processors, you can use the following command to enable per-session accounting for each NP6 processor in the FortiGate unit. Per session accounting is a logging feature that allows the FortiGate to report the correct bytes/pkt numbers per session for sessions offloaded to an NP6 processor. Per-session accounting is not enabled by default because it reduces NP6 offloading performance. So you should only enable per-session accounting if you need the accounting information.

Some FortiOS versions enable per-session-accounting automatically if you enable traffic logging in a firewall policy that allows traffic to pass through an interface attached to an NP6 processor.

Enabling per-session accounting only supports traffic log messages and does not provide traffic flow data for sFlow or NetFlow.

For example, to enable session accounting for the first and second NP6 processors (np6_0 and np6_1):

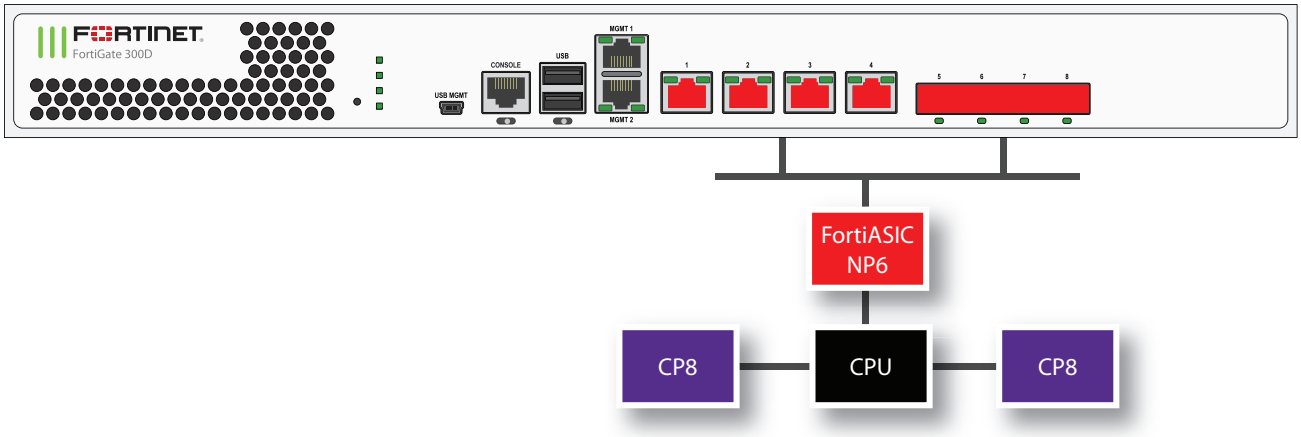
```
config system np6
   edit np6_0
      set per-session-accounting enable
   next
   edit np6_1
      set per-session-accounting enable
   end
```

FortiGate NP6 architectures

Many FortiGate models can offload some types of network traffic processing from main processing resources to specialized network processors. If your network has a significant volume of traffic that is suitable for offloading, this hardware acceleration can significantly improve your network throughput.

FortiGate-300D fast path architecture

The FortiGate-300D includes one NP6 processor connected to four 1Gb RJ-45 Ethernet ports (port1-4) and four 1Gb SFP interfaces (port5-port8).

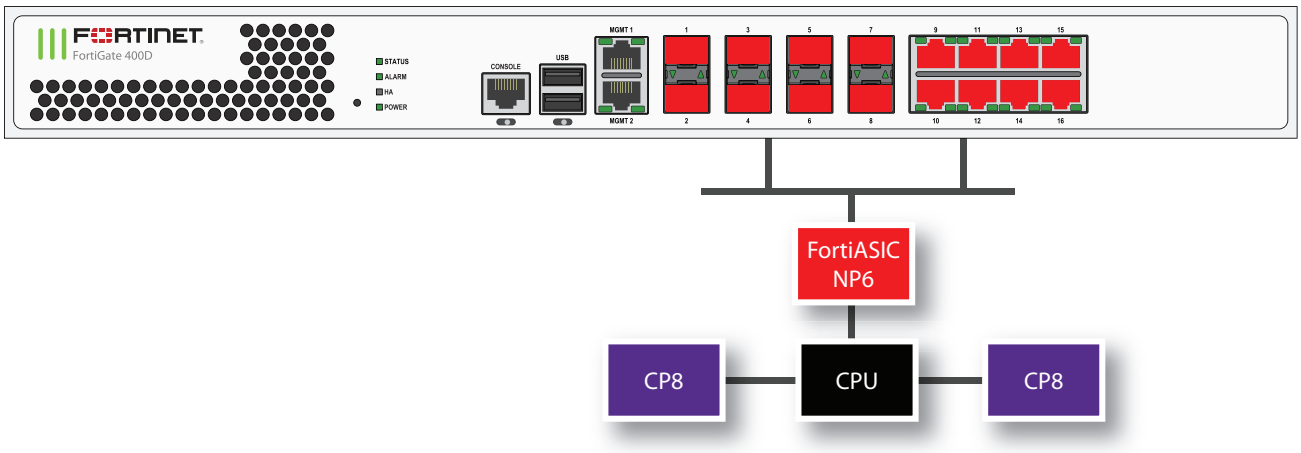


You can use the following command to display the FortiGate-300D NP6 configuration. The command output shows one NP6 named NP6_0 and the interfaces (ports) connected to it.

```
diagnose npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                      Speed offloading
------ ---- ------- ----- ----------
np6_0   0
        1    port5   1G    Yes
        1    port7   1G    Yes
        1    port8   1G    Yes
        1    port6   1G    Yes
        1    port3   1G    Yes
        1    port4   1G    Yes
        1    port1   1G    Yes
        1    port2   1G    Yes
        2
        3
------ ---- ------- ----- ----------
```

FortiGate-400D fast path architecture

The FortiGate-400D includes one NP6 processor connected to eight 1Gb SFP interfaces (port1-port8) and eight 1Gb RJ-45 Ethernet ports (port9-16).

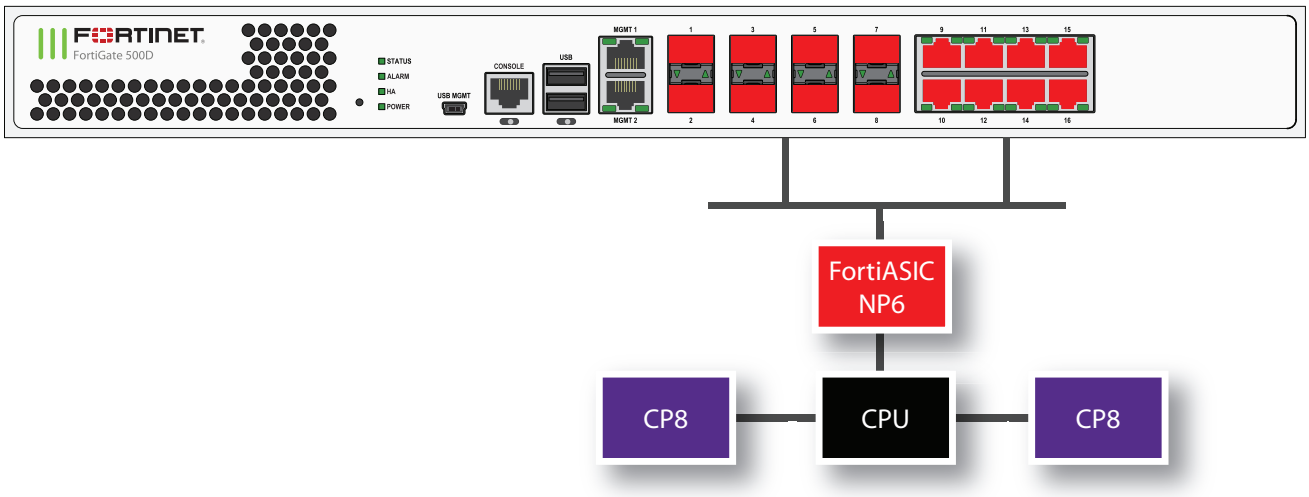


You can use the following command to display the FortiGate-400D NP6 configuration. The command output shows one NP6 named NP6_0 and the interfaces (ports) connected to it.

```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0
       1    port10  1G    Yes
       1    port9   1G    Yes
       1    port12  1G    Yes
       1    port11  1G    Yes
       1    port14  1G    Yes
       1    port13  1G    Yes
       1    port16  1G    Yes
       1    port15  1G    Yes
       1    port5   1G    Yes
       1    port7   1G    Yes
       1    port8   1G    Yes
       1    port6   1G    Yes
       1    port3   1G    Yes
       1    port4   1G    Yes
       1    port1   1G    Yes
       1    port2   1G    Yes
       2
       3
------ ---- ------- ----- ----------
```

FortiGate-500D fast path architecture

The FortiGate-500D includes one NP6 processor connected to eight 1Gb SFP interfaces (port1-port8) and eight 1Gb RJ-45 Ethernet ports (port9-16).

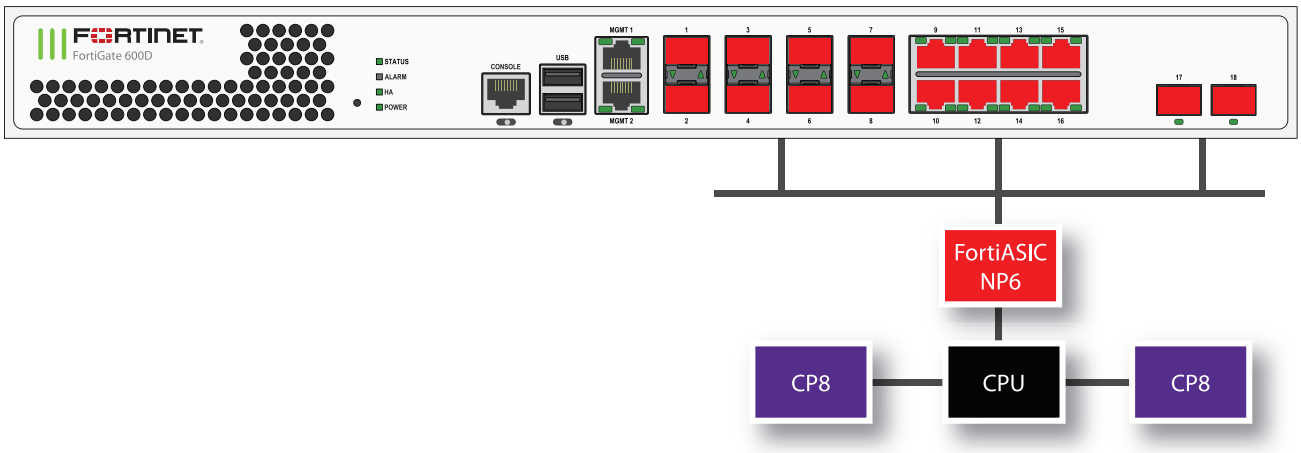


You can use the following command to display the FortiGate-500D NP6 configuration. The command output shows one NP6 named NP6_0 and the interfaces (ports) connected to it.

```
diagnose npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                     Speed offloading
------ ---- ------- ----- ----------
np6_0  0
        1    port10  1G    Yes
        1    port9   1G    Yes
        1    port12  1G    Yes
        1    port11  1G    Yes
        1    port14  1G    Yes
        1    port13  1G    Yes
        1    port16  1G    Yes
        1    port15  1G    Yes
        1    port5   1G    Yes
        1    port7   1G    Yes
        1    port8   1G    Yes
        1    port6   1G    Yes
        1    port3   1G    Yes
        1    port4   1G    Yes
        1    port1   1G    Yes
        1    port2   1G    Yes
        2
        3
------ ---- ------- ----- ----------
```

FortiGate-600D fast path architecture

The FortiGate-600D includes one NP6 processor connected to eight 1Gb SFP interfaces (port1-port8) and eight 1Gb RJ-45 Ethernet ports (port9-16) and two 10Gb SFP+ interfaces (port17 and port18).

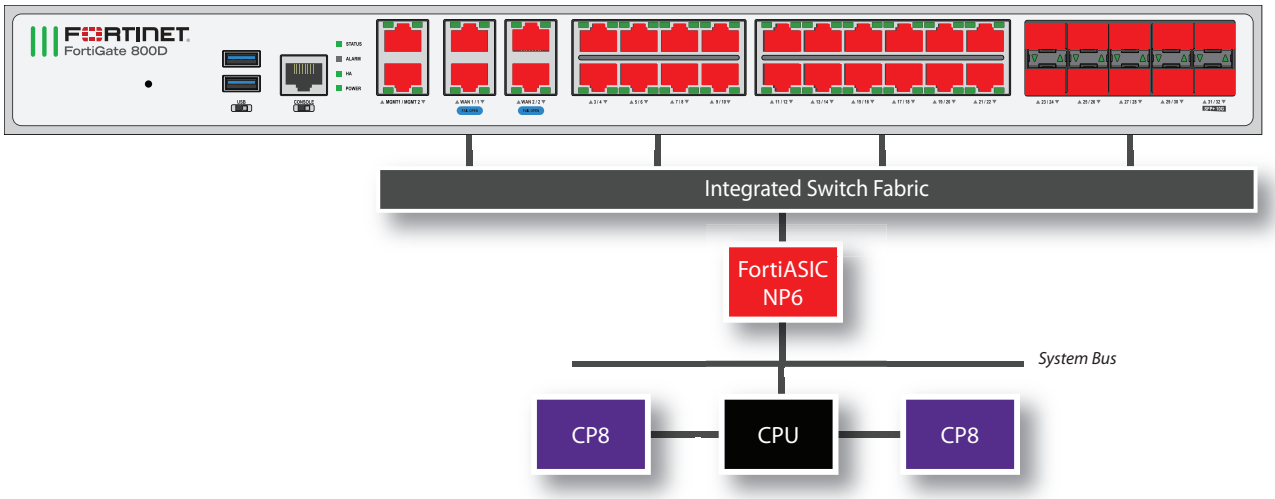


You can use the following command to display the FortiGate-600D NP6 configuration. The command output shows one NP6 named NP6_0 and the interfaces (ports) connected to it.

```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0
       1    port10  1G    Yes
       1    port9   1G    Yes
       1    port12  1G    Yes
       1    port11  1G    Yes
       1    port14  1G    Yes
       1    port13  1G    Yes
       1    port16  1G    Yes
       1    port15  1G    Yes
       1    port5   1G    Yes
       1    port7   1G    Yes
       1    port8   1G    Yes
       1    port6   1G    Yes
       1    port3   1G    Yes
       1    port4   1G    Yes
       1    port1   1G    Yes
       1    port2   1G    Yes
       2    port17  10G   Yes
       3    port18  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-800D fast path architecture

The FortiGate-800D includes one NP6 processor connected through an integrated switch fabric to all of the FortiGate-800D network interfaces. This hardware configuration supports NP6-accelerated fast path offloading for sessions between any of the FortiGate-800D interfaces.



You can use the following diagnose command to display the FortiGate-800D NP6 configuration. The command output shows one NP6 named NP6_0. The output also shows all of the FortiGate-800D interfaces (ports) connected to NP6_0.

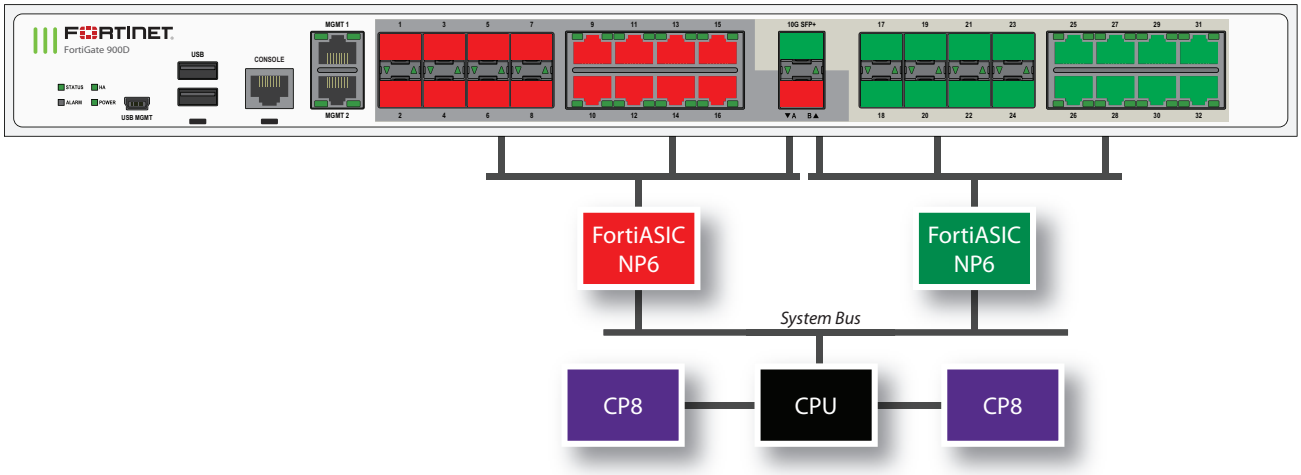
```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0    port31  10G   Yes
       1    wan1    1G    Yes
       1    port1   1G    Yes
       1    wan2    1G    Yes
       1    port2   1G    Yes
       1    port3   1G    Yes
       1    port4   1G    Yes
       1    port5   1G    Yes
       1    port6   1G    Yes
       1    port30  1G    Yes
       1    port29  1G    Yes
       1    port28  1G    Yes
       1    port27  1G    Yes
       1    port26  1G    Yes
       1    port25  1G    Yes
       1    port24  1G    Yes
       1    port23  1G    Yes
       2    port7   1G    Yes
       2    port8   1G    Yes
       2    port9   1G    Yes
       2    port10  1G    Yes
       2    port11  1G    Yes
       2    port12  1G    Yes
       2    port13  1G    Yes
       2    port14  1G    Yes
       2    port15  1G    Yes
       2    port16  1G    Yes
       2    port17  1G    Yes
       2    port18  1G    Yes
       2    port19  1G    Yes
       2    port20  1G    Yes
       2    port21  1G    Yes
       2    port22  1G    Yes
       3    port32  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-900D fast path architecture

The FortiGate-900D includes two NP6 processors that are not connected by an integrated switch fabric (ISF). Without an ISF, traffic through a FortiGate-900D could experience lower latency than traffic through similar hardware with an ISF. The NP6 processors are connected to network interfaces as follows:

Because the FortiGate-900D does not have an ISF you cannot create Link Aggregation Groups (LAGs) that include interfaces connected to both NP6 processors.

- Eight 1Gb SFP interfaces (port17-port24), eight 1Gb RJ-45 Ethernet interfaces (port25-32) and one 10Gb SFP+ interface (portB) share connections to the first NP6 processor.
- Eight 1Gb SFP interfaces (port1-port8), eight RJ-45 Ethernet interfaces (port9-16) and one 10Gb SFP+ interface (portA) share connections to the second NP6 processor.



You can use the following command to display the FortiGate-900D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

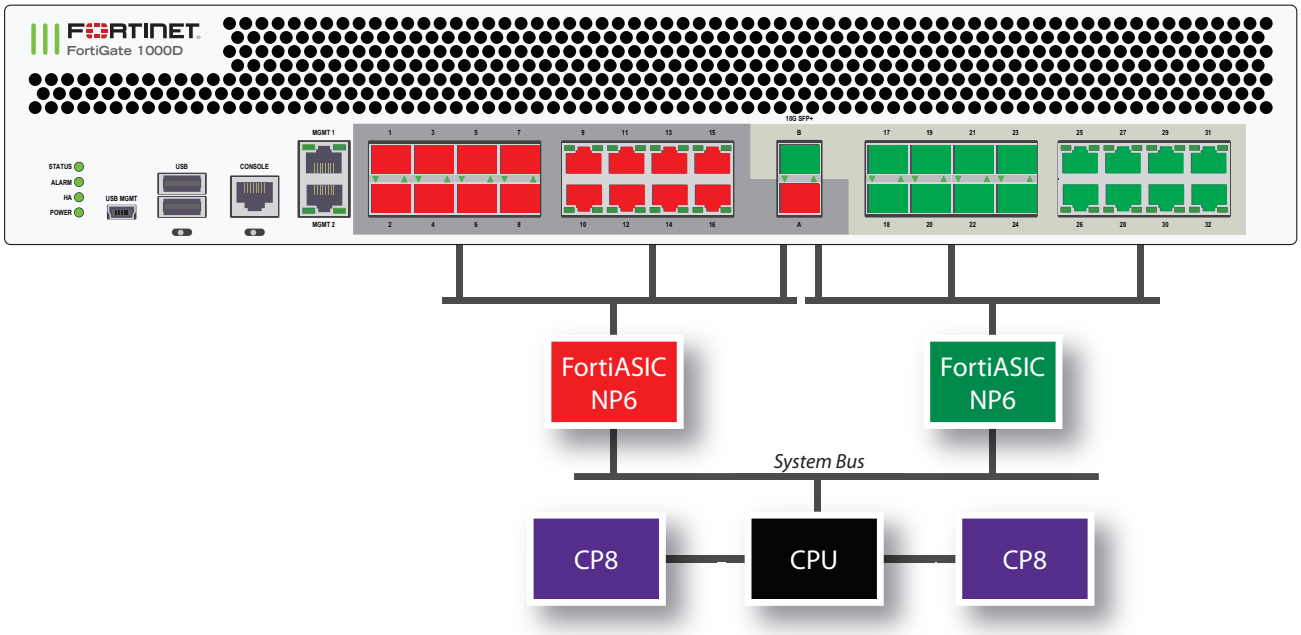
```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0
       1    port17  1G    Yes
       1    port18  1G    Yes
       1    port19  1G    Yes
       1    port20  1G    Yes
       1    port21  1G    Yes
       1    port22  1G    Yes
       1    port23  1G    Yes
       1    port24  1G    Yes
       1    port27  1G    Yes
       1    port28  1G    Yes
       1    port25  1G    Yes
       1    port26  1G    Yes
       1    port31  1G    Yes
       1    port32  1G    Yes
       1    port29  1G    Yes
       1    port30  1G    Yes
       2    portB   10G   Yes
       3
------ ---- ------- ----- ----------
np6_1   0
        1    port1  1G    Yes
        1    port2  1G    Yes
        1    port3  1G    Yes
        1    port4  1G    Yes
        1    port5  1G    Yes
        1    port6  1G    Yes
        1    port7  1G    Yes
        1    port8  1G    Yes
        1    port11 1G    Yes
        1    port12 1G    Yes
        1    port9  1G    Yes
        1    port10 1G    Yes
        1    port15 1G    Yes
        1    port16 1G    Yes
        1    port13 1G    Yes
        1    port14 1G    Yes
        2    portA  10G   Yes
        3
```

FortiGate-1000D fast path architecture

The FortiGate-1000D includes two NP6 processors that are not connected by an integrated switch fabric (ISF). The NP6 processors are connected to network interfaces as follows:

Because the FortiGate-1000D does not have an ISF you cannot create Link Aggregation Groups (LAGs) that include interfaces connected to both NP6 processors.

- Eight 1Gb SFP interfaces (port17-port24), eight 1Gb RJ-45 Ethernet interfaces (port25-32) and one 10Gb SFP+ interface (portB) share connections to the first NP6 processor.
- Eight 1Gb SFP interfaces (port1-port8), eight RJ-45 Ethernet interfaces (port9-16) and one 10Gb SFP+ interface (portA) share connections to the second NP6 processor.



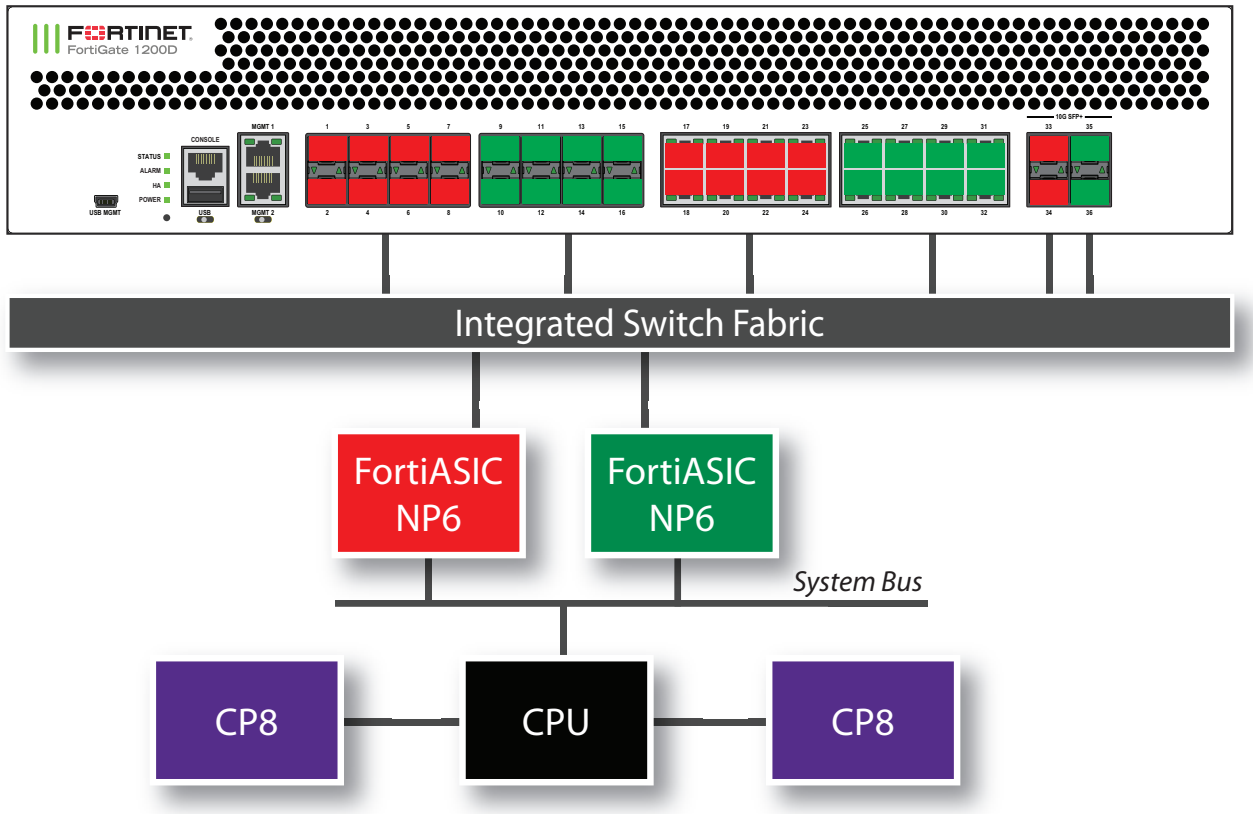
You can use the following command to display the FortiGate-1000D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0
       1    port17  1G    Yes
       1    port18  1G    Yes
       1    port19  1G    Yes
       1    port20  1G    Yes
       1    port21  1G    Yes
       1    port22  1G    Yes
       1    port23  1G    Yes
       1    port24  1G    Yes
       1    port27  1G    Yes
       1    port28  1G    Yes
       1    port25  1G    Yes
       1    port26  1G    Yes
       1    port31  1G    Yes
       1    port32  1G    Yes
       1    port29  1G    Yes
       1    port30  1G    Yes
       2    portB   10G   Yes
       3
------ ---- ------- ----- ----------
np6_1   0
        1    port1  1G    Yes
        1    port2  1G    Yes
        1    port3  1G    Yes
        1    port4  1G    Yes
        1    port5  1G    Yes
        1    port6  1G    Yes
        1    port7  1G    Yes
        1    port8  1G    Yes
        1    port11 1G    Yes
        1    port12 1G    Yes
        1    port9  1G    Yes
        1    port10 1G    Yes
        1    port15 1G    Yes
        1    port16 1G    Yes
        1    port13 1G    Yes
        1    port14 1G    Yes
        2    portA  10G   Yes
        3
```

FortiGate-1200D fast path architecture

The FortiGate-1200D features two NP6 processors both connected to an integrated switch fabric.

- Eight SFP 1Gb interfaces (port1-port8), eight RJ-45 Ethernet ports (port17-24) and two SFP+ 10Gb interfaces (port33 and port34) share connections to the first NP6 processor.
- Eight SFP 1Gb interfaces (port9-port16), eight RJ-45 Ethernet ports (port25-32) and two SFP+ 10Gb interfaces (port35-port36) share connections to the second NP6 processor.



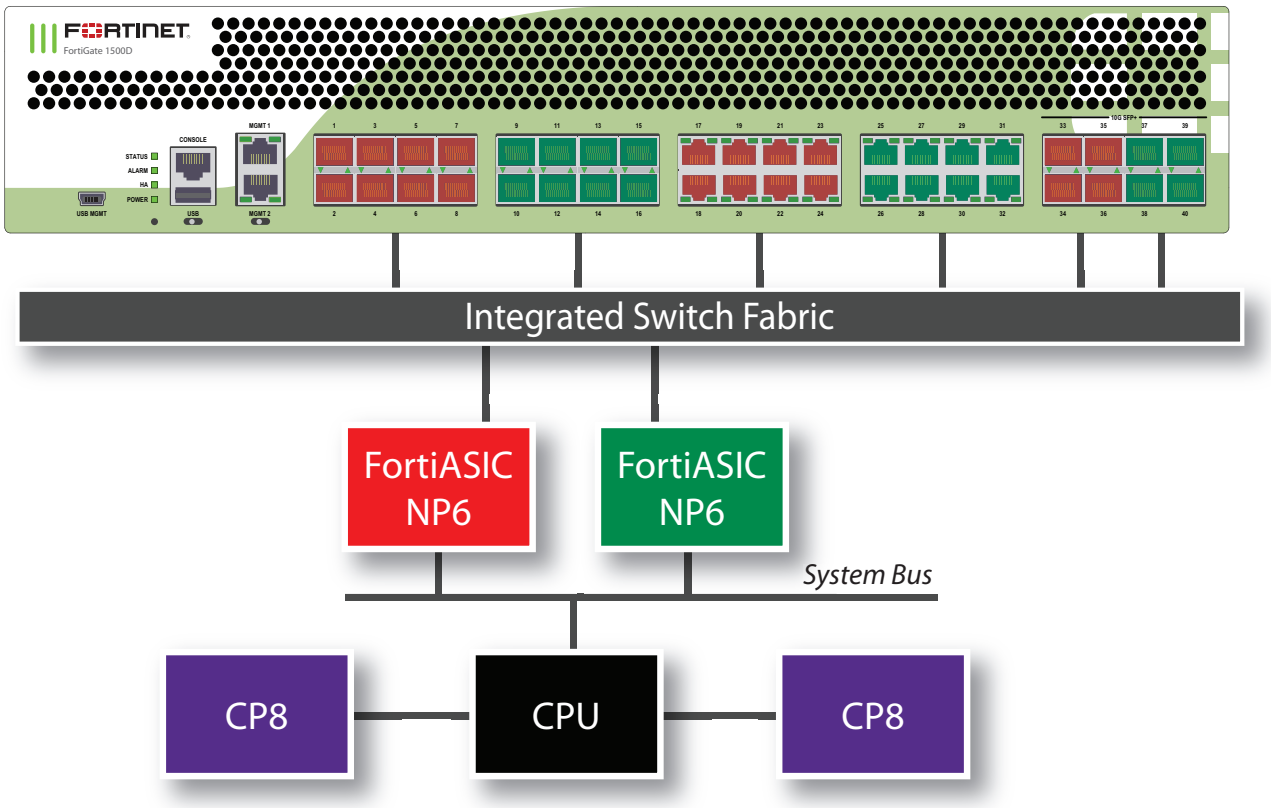
You can use the following command to display the FortiGate-1200D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_0  0    port33  10G   Yes
       1    port34  10G   Yes
       2    port1   1G    Yes
       2    port3   1G    Yes
       2    port5   1G    Yes
       2    port7   1G    Yes
       2    port17  1G    Yes
       2    port19  1G    Yes
       2    port21  1G    Yes
       2    port23  1G    Yes
       3    port2   1G    Yes
       3    port4   1G    Yes
       3    port6   1G    Yes
       3    port8   1G    Yes
       3    port18  1G    Yes
       3    port20  1G    Yes
       3    port22  1G    Yes
       3    port24  1G    Yes
------ ---- ------- ----- ----------
np6_1  0    port35  10G   Yes
       1    port36  10G   Yes
       2    port9   1G    Yes
       2    port11  1G    Yes
       2    port13  1G    Yes
       2    port15  1G    Yes
       2    port25  1G    Yes
       2    port27  1G    Yes
       2    port29  1G    Yes
       2    port31  1G    Yes
       3    port10  1G    Yes
       3    port12  1G    Yes
       3    port14  1G    Yes
       3    port16  1G    Yes
       3    port26  1G    Yes
       3    port28  1G    Yes
       3    port30  1G    Yes
       3    port32  1G    Yes
------ ---- ------- ----- ----------
```

FortiGate-1500D fast path architecture

The FortiGate-1500D features two NP6 processors both connected to an integrated switch fabric.

- Eight SFP 1Gb interfaces (port1-port8), eight RJ-45 Ethernet ports (port17-24) and four SFP+ 10Gb interfaces (port33-port36) share connections to the first NP6 processor.
- Eight SFP 1Gb interfaces (port9-port16), eight RJ-45 Ethernet ports (port25-32) and four SFP+ 10Gb interfaces (port37-port40) share connections to the second NP6 processor.



You can use the following diagnose command to display the FortiGate-1500D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip    XAUI Ports             Max    Cross-chip
                               Speed offloading
------  ---- -------           -----  ----------
np6_0   0    port1             1G     Yes
        0    port5             1G     Yes
        0    port17            1G     Yes
        0    port21            1G     Yes
        0    port33            10G    Yes
        1    port2             1G     Yes
        1    port6             1G     Yes
        1    port18            1G     Yes
        1    port22            1G     Yes
```

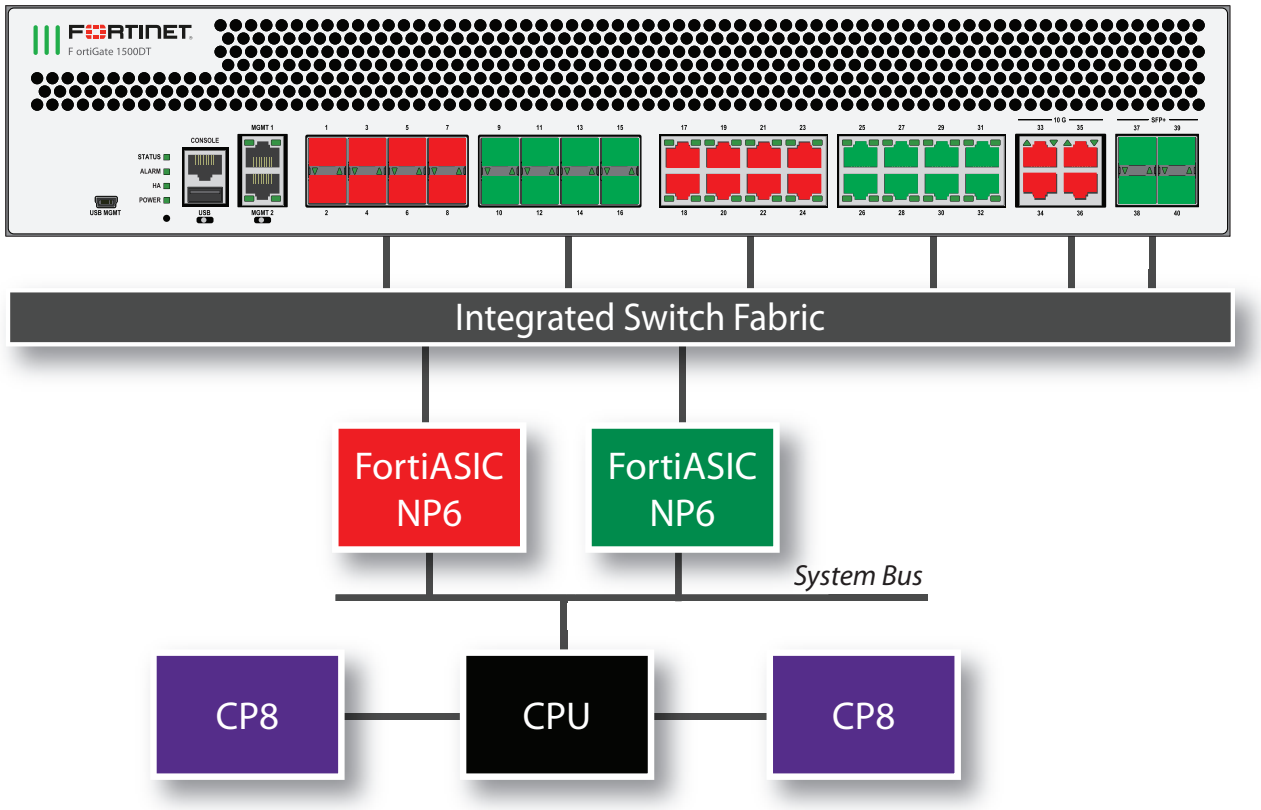
```
        1    port34           10G   Yes
        2    port3            1G    Yes
        2    port7            1G    Yes
        2    port19           1G    Yes
        2    port23           1G    Yes
        2    port35           10G   Yes
        3    port4            1G    Yes
        3    port8            1G    Yes
        3    port20           1G    Yes
        3    port24           1G    Yes
        3    port36           10G   Yes
------ ---- -------          ----- ----------
np6_1  0    port9            1G    Yes
       0    port13           1G    Yes
       0    port25           1G    Yes
       0    port29           1G    Yes
       0    port37           10G   Yes
       1    port10           1G    Yes
       1    port14           1G    Yes
       1    port26           1G    Yes
       1    port30           1G    Yes
       1    port38           10G   Yes
       2    port11           1G    Yes
       2    port15           1G    Yes
       2    port27           1G    Yes
       2    port31           1G    Yes
       2    port39           10G   Yes
       3    port12           1G    Yes
       3    port16           1G    Yes
       3    port28           1G    Yes
       3    port32           1G    Yes
       3    port40           10G   Yes
------ ---- -------          ----- ----------
```

FortiGate-1500DT fast path architecture

The FortiGate-1500DT features two NP6 processors both connected to an integrated switch fabric. The FortiGate-1500DT has the same hardware configuration as the FortiGate-1500D, but with the addition of newer CPUs and DPDK technology that improves IPS performance.

The FortiGate-1500DT includes the following interfaces and NP6 processors:

- Eight SFP 1Gb interfaces (port1-port8), eight RJ-45 Ethernet ports (port17-24) and four SFP+ 10Gb interfaces (port33-port36) share connections to the first NP6 processor.
- Eight SFP 1Gb interfaces (port9-port16), eight RJ-45 Ethernet ports (port25-32) and four SFP+ 10Gb interfaces (port37-port40) share connections to the second NP6 processor.



You can use the following diagnose command to display the FortiGate-1500DT NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

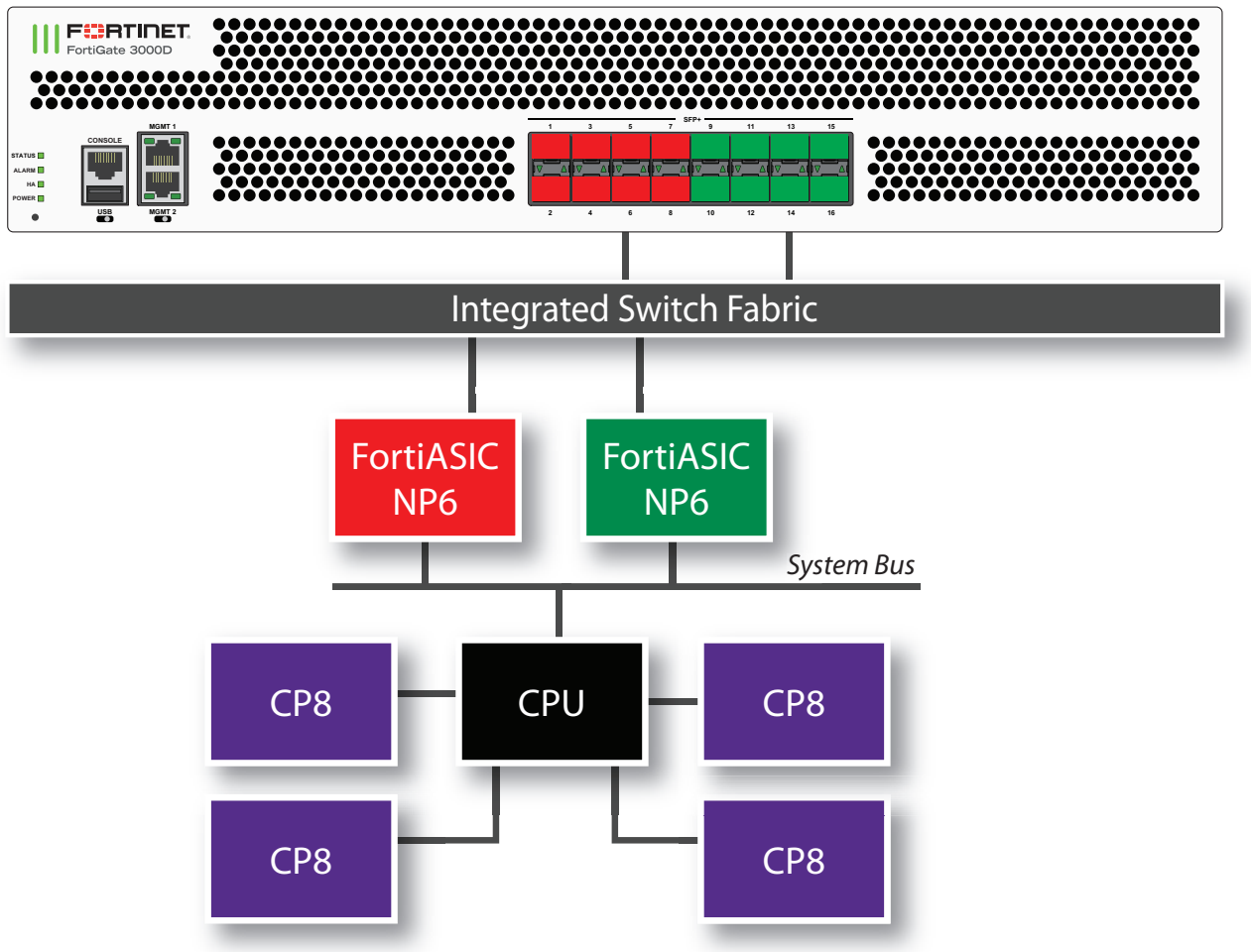
```
diagnose npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                      Speed  offloading
------  ---- -------  -----  ----------
np6_0   0    port1    1G     Yes
        0    port5    1G     Yes
        0    port17   1G     Yes
        0    port21   1G     Yes
        0    port33   10G    Yes
        1    port2    1G     Yes
        1    port6    1G     Yes
        1    port18   1G     Yes
        1    port22   1G     Yes
        1    port34   10G    Yes
        2    port3    1G     Yes
        2    port7    1G     Yes
        2    port19   1G     Yes
        2    port23   1G     Yes
        2    port35   10G    Yes
        3    port4    1G     Yes
        3    port8    1G     Yes
        3    port20   1G     Yes
        3    port24   1G     Yes
```

```
        3    port36  10G   Yes
------ ---- ------- ----- ----------
np6_1  0    port9   1G    Yes
       0    port13  1G    Yes
       0    port25  1G    Yes
       0    port29  1G    Yes
       0    port37  10G   Yes
       1    port10  1G    Yes
       1    port14  1G    Yes
       1    port26  1G    Yes
       1    port30  1G    Yes
       1    port38  10G   Yes
       2    port11  1G    Yes
       2    port15  1G    Yes
       2    port27  1G    Yes
       2    port31  1G    Yes
       2    port39  10G   Yes
       3    port12  1G    Yes
       3    port16  1G    Yes
       3    port28  1G    Yes
       3    port32  1G    Yes
       3    port40  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-3000D fast path architecture

The FortiGate-3000D features 16 front panel SFP+ 10Gb interfaces connected to two NP6 processors through an Integrated Switch Fabirc (ISF). The FortiGate-3000D has the following fastpath architecture:

- 8 SFP+ 10Gb interfaces, port1 through port8 share connections to the first NP6 processor (np6_0).
- 8 SFP+ 10Gb interfaces, port9 through port16 share connections to the second NP6 processor (np6_1).



You can use the following command to display the FortiGate-3000D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1 and the interfaces (ports) connected to each NP6.

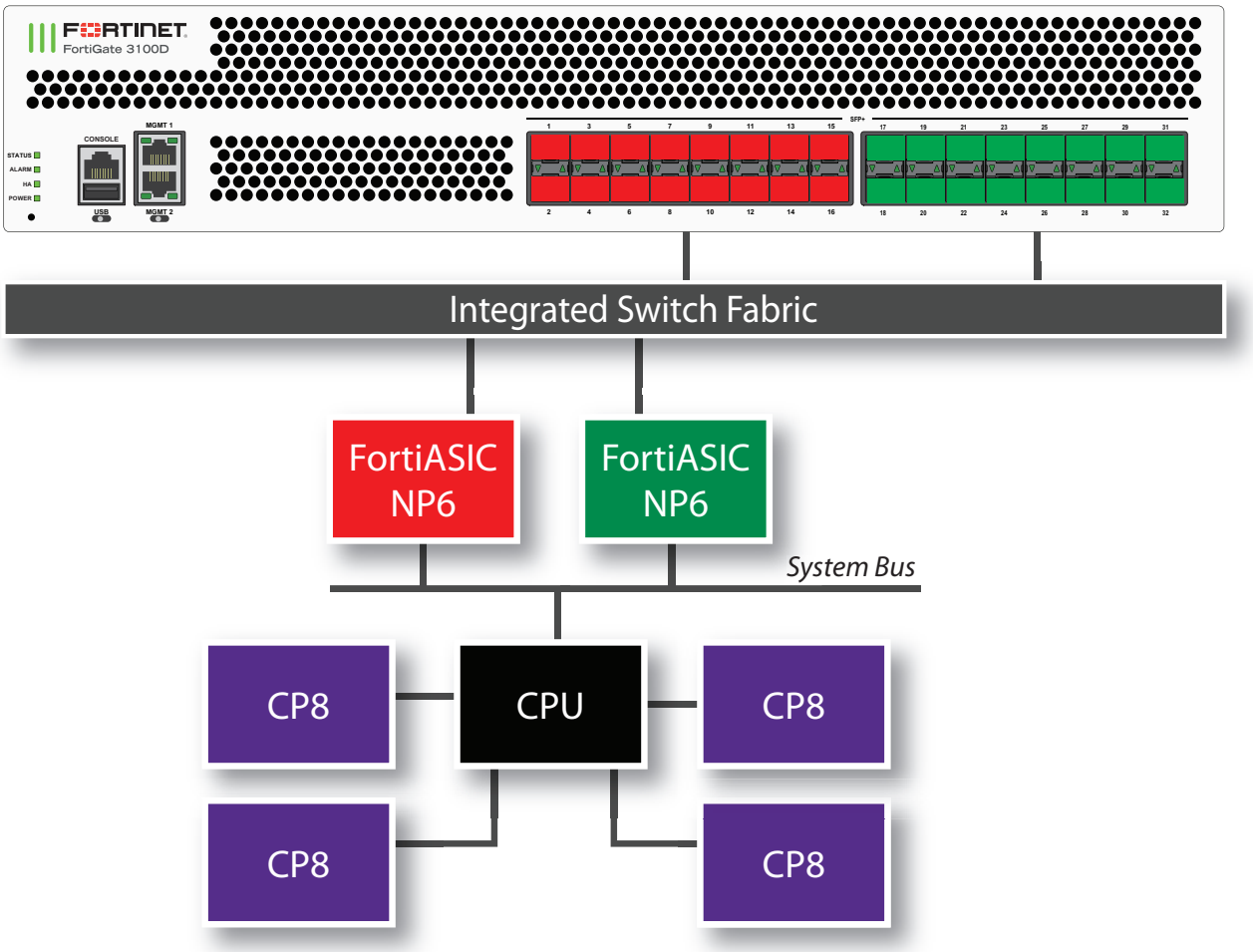
```
dia npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                      Speed  offloading
------  ---- -------  -----  ----------
np6_0   0    port1    10G    Yes
        0    port6    10G    Yes
        1    port2    10G    Yes
        1    port5    10G    Yes
        2    port3    10G    Yes
        2    port8    10G    Yes
        3    port4    10G    Yes
        3    port7    10G    Yes
------  ---- -------  -----  ----------
np6_1   0    port10   10G    Yes
        0    port13   10G    Yes
        1    port9    10G    Yes
        1    port14   10G    Yes
        2    port12   10G    Yes
        2    port15   10G    Yes
```

```
        3    port11  10G   Yes
        3    port16  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-3100D fast path architecture

The FortiGate-3100D features 32 SFP+ 10Gb interfaces connected to two NP6 processors through an Integrated Switch Fabirc (ISF). The FortiGate-3100D has the following fastpath architecture:

- 16 SFP+ 10Gb interfaces, port1 through port16 share connections to the first NP6 processor (np6_0).
- 16 SFP+ 10Gb interfaces, port27 through port32 share connections to the second NP6 processor (np6_1).



You can use the following command to display the FortiGate-3100D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1 and the interfaces (ports) connected to each NP6.

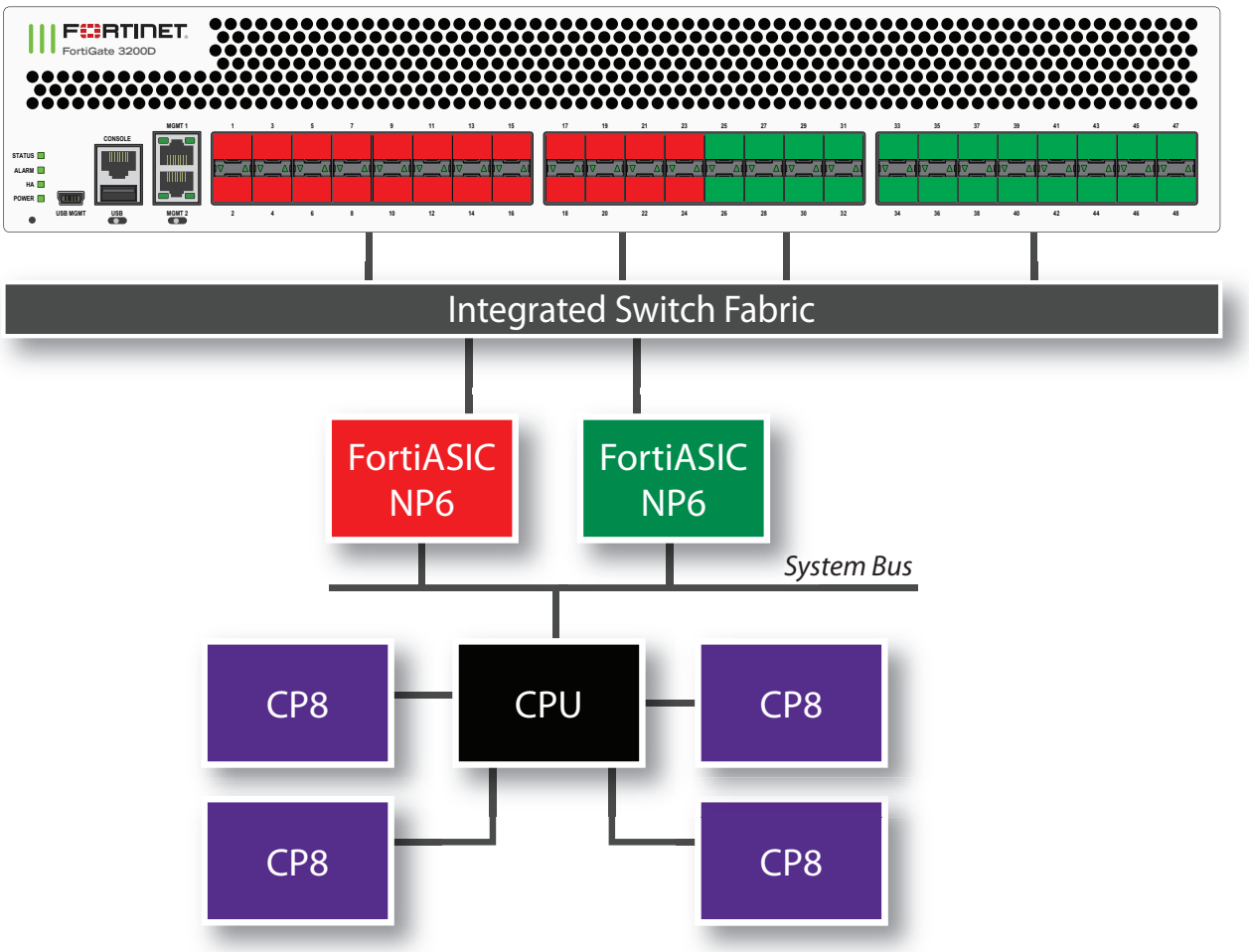
```
diag npu np6 port-list
Chip    XAUI Ports   Max   Cross-chip
                     Speed offloading
------ ---- ------- ----- ----------
np6_0   0    port1   10G   Yes
        0    port6   10G   Yes
        0    port10  10G   Yes
```

```
        0    port13  10G   Yes
        1    port2   10G   Yes
        1    port5   10G   Yes
        1    port9   10G   Yes
        1    port14  10G   Yes
        2    port3   10G   Yes
        2    port8   10G   Yes
        2    port12  10G   Yes
        2    port15  10G   Yes
        3    port4   10G   Yes
        3    port7   10G   Yes
        3    port11  10G   Yes
        3    port16  10G   Yes
------ ---- ------- ----- ----------
np6_1  0    port17  10G   Yes
        0    port21  10G   Yes
        0    port25  10G   Yes
        0    port29  10G   Yes
        1    port18  10G   Yes
        1    port22  10G   Yes
        1    port26  10G   Yes
        1    port30  10G   Yes
        2    port19  10G   Yes
        2    port23  10G   Yes
        2    port27  10G   Yes
        2    port31  10G   Yes
        3    port20  10G   Yes
        3    port24  10G   Yes
        3    port28  10G   Yes
        3    port32  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-3200D fast path architecture

The FortiGate-3200D features two NP6 processors connected to an Integrated Switch Fabirc (ISF). The FortiGate-3200D has the following fastpath architecture:

- 24 SFP+ 10Gb interfaces, port1 through port24 share connections to the first NP6 processor (np6_0).
- 24 SFP+ 10Gb interfaces, port25 through port48 share connections to the second NP6 processor (np6_1).



You can use the following command to display the FortiGate-3200D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1 and the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                      Speed offloading
------  ---- -------  -----  ----------
np6_0   0    port1    10G    Yes
        0    port5    10G    Yes
        0    port10   10G    Yes
        0    port13   10G    Yes
        0    port17   10G    Yes
        0    port22   10G    Yes
        1    port2    10G    Yes
        1    port6    10G    Yes
        1    port9    10G    Yes
        1    port14   10G    Yes
        1    port18   10G    Yes
        1    port21   10G    Yes
        2    port3    10G    Yes
        2    port7    10G    Yes
        2    port12   10G    Yes
```

```
        2    port15  10G   Yes
        2    port19  10G   Yes
        2    port24  10G   Yes
        3    port4   10G   Yes
        3    port8   10G   Yes
        3    port11  10G   Yes
        3    port16  10G   Yes
        3    port20  10G   Yes
        3    port23  10G   Yes
------ ---- ------- ----- ----------
np6_1  0    port26  10G   Yes
        0    port29  10G   Yes
        0    port33  10G   Yes
        0    port37  10G   Yes
        0    port41  10G   Yes
        0    port45  10G   Yes
        1    port25  10G   Yes
        1    port30  10G   Yes
        1    port34  10G   Yes
        1    port38  10G   Yes
        1    port42  10G   Yes
        1    port46  10G   Yes
        2    port28  10G   Yes
        2    port31  10G   Yes
        2    port35  10G   Yes
        2    port39  10G   Yes
        2    port43  10G   Yes
        2    port47  10G   Yes
        3    port27  10G   Yes
        3    port32  10G   Yes
        3    port36  10G   Yes
        3    port40  10G   Yes
        3    port44  10G   Yes
        3    port48  10G   Yes
------ ---- ------- ----- ----------
```

FortiGate-3700D fast path architecture

The FortiGate-3700D features four NP6 processors.The first two NP6 processors (np6_0 and np6_1) can be configured for low latency operation. The low latency configuration changes the FortiGate-3700D fast path architecture.

FortiGate-3700D low latency fast path architecture

Ports 25 to 32 can be used for low latency offloading. As long as traffic enters and exits the FortiGate-3700D through ports connected to the same NP6 processor and using these low latency ports the traffic will be offloaded and have lower latency that other NP6 offloaded traffic. Latency is reduced by bypassing the integrated switch fabric (ISF).

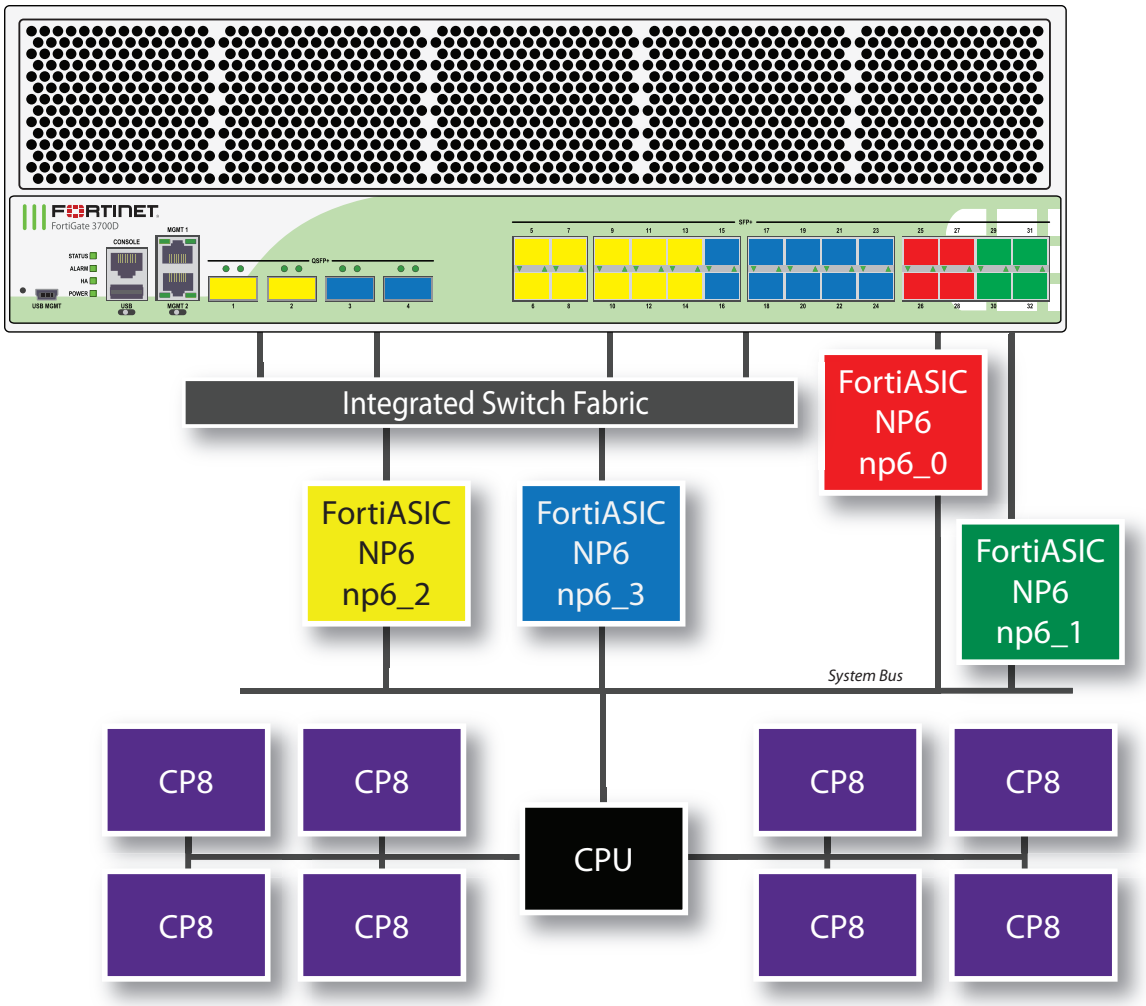
You can use the following command to turn on low latency mode for np6_0 and np6_1:

```
config system np6
   edit np6_0
      set low-latency-mode enable
   next
   edit np6_1
      set low-latency-mode enable
   end
```

You do not have to turn on low latency to both np6_0 and np6_1. If you turn on low latency for just one NP6, the other NP6 will still be mapped according to the normal latency configuration.

With low latency enabled for both np6_0 and np6_1 the FortiGate-3700D has the following fastpath architecture:

- Four SFP+ 10Gb interfaces, port25 to port28, share connections to the first NP6 processor (np6_0) so sessions entering one of these ports and exiting through another will experience low latency
- Four SFP+ 10Gb interfaces, port29 to port32, share connections to the second NP6 processor (np6_1) so sessions entering one of these ports and exiting through another will experience low latency
- Ten SFP+ 10Gb interfaces, port5 to port14, and two 40Gb QSFP interfaces, port1 and port2, share connections to the third NP6 processor (np6_2).
- Ten SFP+ 10Gb interfaces, port15 to port24, and two 40Gb QSFP interfaces, port3 and port4, share connections to the fourth NP6 processor (np6_3).



You can use the following command to display the FortiGate-3700D NP6 configuration. In this output example, the first two NP6s (np6_0 and np6_1) are configured for low latency. The command output shows four NP6s named NP6_0, NP6_1, NP6_2, and NP6_3 and the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                      Speed offloading
------  ---- -------  -----  ----------
np6_2   0    port5    10G    Yes
        0    port9    10G    Yes
        0    port13   10G    Yes
        1    port6    10G    Yes
        1    port10   10G    Yes
        1    port14   10G    Yes
        2    port7    10G    Yes
        2    port11   10G    Yes
        3    port8    10G    Yes
        3    port12   10G    Yes
        0-3  port1    40G    Yes
        0-3  port2    40G    Yes
```

```
------ ---- ------- ----- ----------
np6_3  0    port15  10G   Yes
       0    port19  10G   Yes
       0    port23  10G   Yes
       1    port16  10G   Yes
       1    port20  10G   Yes
       1    port24  10G   Yes
       2    port17  10G   Yes
       2    port21  10G   Yes
       3    port18  10G   Yes
       3    port22  10G   Yes
       0-3  port3   40G   Yes
       0-3  port4   40G   Yes
------ ---- ------- ----- ----------
np6_0  0    port26  10G   No
       1    port25  10G   No
       2    port28  10G   No
       3    port27  10G   No
------ ---- ------- ----- ----------
np6_1  0    port30  10G   No
       1    port29  10G   No
       2    port32  10G   No
       3    port31  10G   No
------ ---- ------- ----- ----------
```

FortiGate-3700D normal latency fast path architecture

You can use the following command to turn off low latency mode for np6_0 and np6_1:

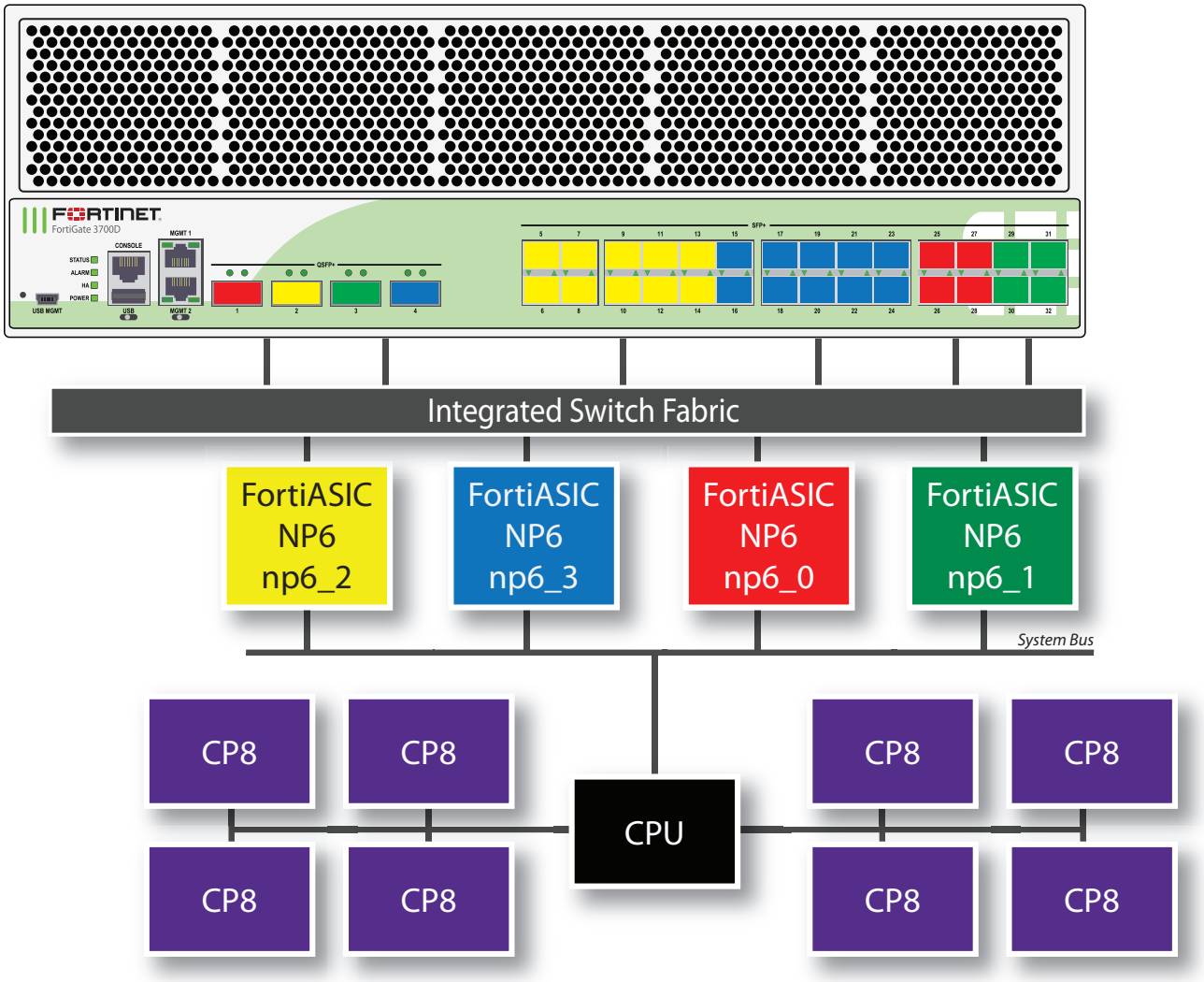
```
config system np6
   edit np6_0
      set low-latency-mode disable
   next
   edit np6_1
      set low-latency-mode disable
   end
```

You do not have to turn off low latency to both np6_0 and np6_1. If you turn off low latency to just one NP6, the other NP6 will still be mapped according to the normal configuration.

In addition to turning off low latency, entering these commands also changes how ports are mapped to NP6s. Port1 is now mapped to np6_0 and port 3 is not mapped to np6_1. The FortiGate-3700D has the following fastpath architecture:

- One 40Gb QSFP interface, port1, and four SFP+ 10Gb interfaces, port25 to port28 share connections to the first NP6 processor (np6_0).
- One 40Gb QSFP interface, port3, and four SFP+ 10Gb interfaces, port29 to port32 share connections to the second NP6 processor (np6_1).
- One 40Gb QSFP interface, port2 and ten SFP+ 10Gb interfaces, port5 to port14 share connections to the third NP6 processor (np6_2).

- One 40Gb QSFP interface, port4, and ten SFP+ 10Gb interfaces, port15 to port24 share connections to the fourth NP6 processor (np6_3).



You can use the following command to display the FortiGate-3700D NP6 configuration with low latency turned off for np6_0 and np6_1. The command output shows four NP6s named NP6_0, NP6_1, NP6_2, and NP6_3 and the interfaces (ports) connected to each NP6.

```
dia npu np6 port-list
Chip   XAUI Ports            Max   Cross-chip
                             Speed offloading
------ ---- -------          ----- ----------
np6_0  0    port26           10G   Yes
       1    port25           10G   Yes
       2    port28           10G   Yes
       3    port27           10G   Yes
       0-3  port1            40G   Yes
------ ---- -------          ----- ----------
np6_1  0    port30           10G   Yes
       1    port29           10G   Yes
       2    port32           10G   Yes
```

```
        3    port31           10G   Yes
        0-3  port3            40G   Yes
------ ---- -------          ----- ----------
np6_2   0    port5            10G   Yes
        0    port9            10G   Yes
        0    port13           10G   Yes
        1    port6            10G   Yes
        1    port10           10G   Yes
        1    port14           10G   Yes
        2    port7            10G   Yes
        2    port11           10G   Yes
        3    port8            10G   Yes
        3    port12           10G   Yes
        0-3  port2            40G   Yes
------ ---- -------          ----- ----------
np6_3   0    port15           10G   Yes
        0    port19           10G   Yes
        0    port23           10G   Yes
        1    port16           10G   Yes
        1    port20           10G   Yes
        1    port24           10G   Yes
        2    port17           10G   Yes
        2    port21           10G   Yes
        3    port18           10G   Yes
        3    port22           10G   Yes
        0-3  port4            40G   Yes
------ ---- -------          ----- ----------
```

FortiGate-3700DX fast path architecture

The FortiGate-3700DX features four NP6 processors.The first two NP6 processors (np6_0 and np6_1) can be configured for low latency operation. The low latency configuration changes the FortiGate-3700DX fast path architecture. The FortiGate-3700DX also includes two TP2 cards that are not supported by FortiOS 5.2.

FortiGate-3700DX low latency fast path architecture

Ports 25 to 32 can be used for low latency offloading. As long as traffic enters and exits the FortiGate-3700DX through ports connected to the same NP6 processor and using these low latency ports the traffic will be offloaded and have lower latency that other NP6 offloaded traffic. Latency is reduced by bypassing the integrated switch fabric (ISF).

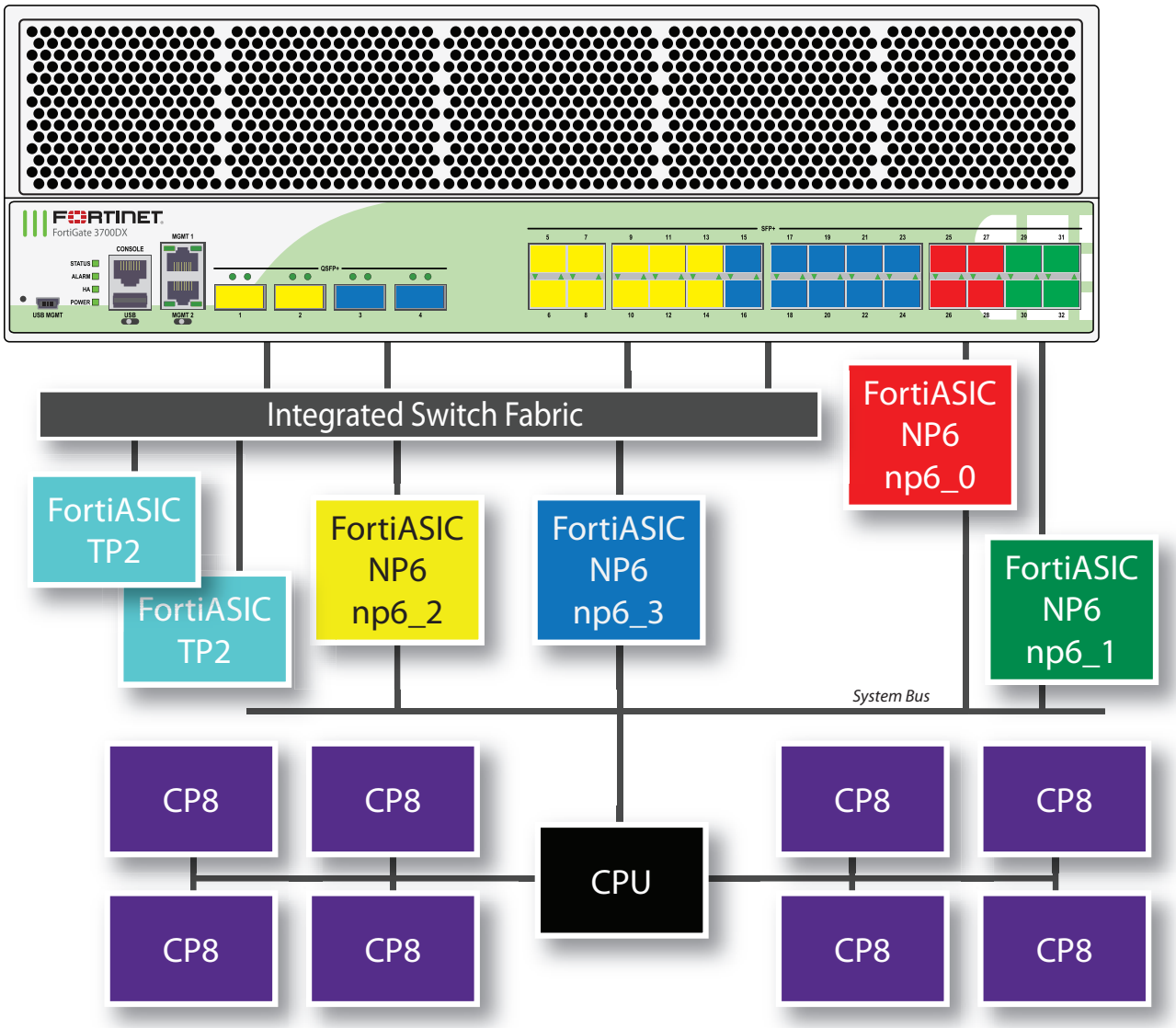
You can use the following command to turn on low latency mode for np6_0 and np6_1:

```
config system np6
  edit np6_0
    set low-latency-mode enable
  next
  edit np6_1
    set low-latency-mode enable
  end
```

You do not have to turn on low latency to both np6_0 and np6_1. If you turn on low latency for just one NP6, the other NP6 will still be mapped according to the normal latency configuration.

With low latency enabled for both np6_0 and np6_1 the FortiGate-3700DX has the following fastpath architecture:

- Four SFP+ 10Gb interfaces, port25 to port28, share connections to the first NP6 processor (np6_0) so sessions entering one of these ports and exiting through another will experience low latency
- Four SFP+ 10Gb interfaces, port29 to port32, share connections to the second NP6 processor (np6_1) so sessions entering one of these ports and exiting through another will experience low latency
- Ten SFP+ 10Gb interfaces, port5 to port14, and two 40Gb QSFP interfaces, port1 and port2, share connections to the third NP6 processor (np6_2).
- Ten SFP+ 10Gb interfaces, port15 to port24, and two 40Gb QSFP interfaces, port3 and port4, share connections to the fourth NP6 processor (np6_3).



You can use the following diagnose command to display the FortiGate-3700DX NP6 configuration. In this output example, the first two NP6s (np6_0 and np6_1) are configured for low latency. The command output shows four NP6s named NP6_0, NP6_1, NP6_2, and NP6_3 and the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip   XAUI Ports   Max   Cross-chip
                    Speed offloading
------ ---- ------- ----- ----------
np6_2  0    port5   10G   Yes
       0    port9   10G   Yes
       0    port13  10G   Yes
       1    port6   10G   Yes
       1    port10  10G   Yes
       1    port14  10G   Yes
       2    port7   10G   Yes
       2    port11  10G   Yes
       3    port8   10G   Yes
       3    port12  10G   Yes
       0-3  port1   40G   Yes
       0-3  port2   40G   Yes
------ ---- ------- ----- ----------
np6_3  0    port15  10G   Yes
       0    port19  10G   Yes
       0    port23  10G   Yes
       1    port16  10G   Yes
       1    port20  10G   Yes
       1    port24  10G   Yes
       2    port17  10G   Yes
       2    port21  10G   Yes
       3    port18  10G   Yes
       3    port22  10G   Yes
       0-3  port3   40G   Yes
       0-3  port4   40G   Yes
------ ---- ------- ----- ----------
np6_0  0    port26  10G   No
       1    port25  10G   No
       2    port28  10G   No
       3    port27  10G   No
------ ---- ------- ----- ----------
np6_1  0    port30  10G   No
       1    port29  10G   No
       2    port32  10G   No
       3    port31  10G   No
------ ---- ------- ----- ----------
```

FortiGate-3700DX normal latency fast path architecture

You can use the following command to turn off low latency mode for np6_0 and np6_1:

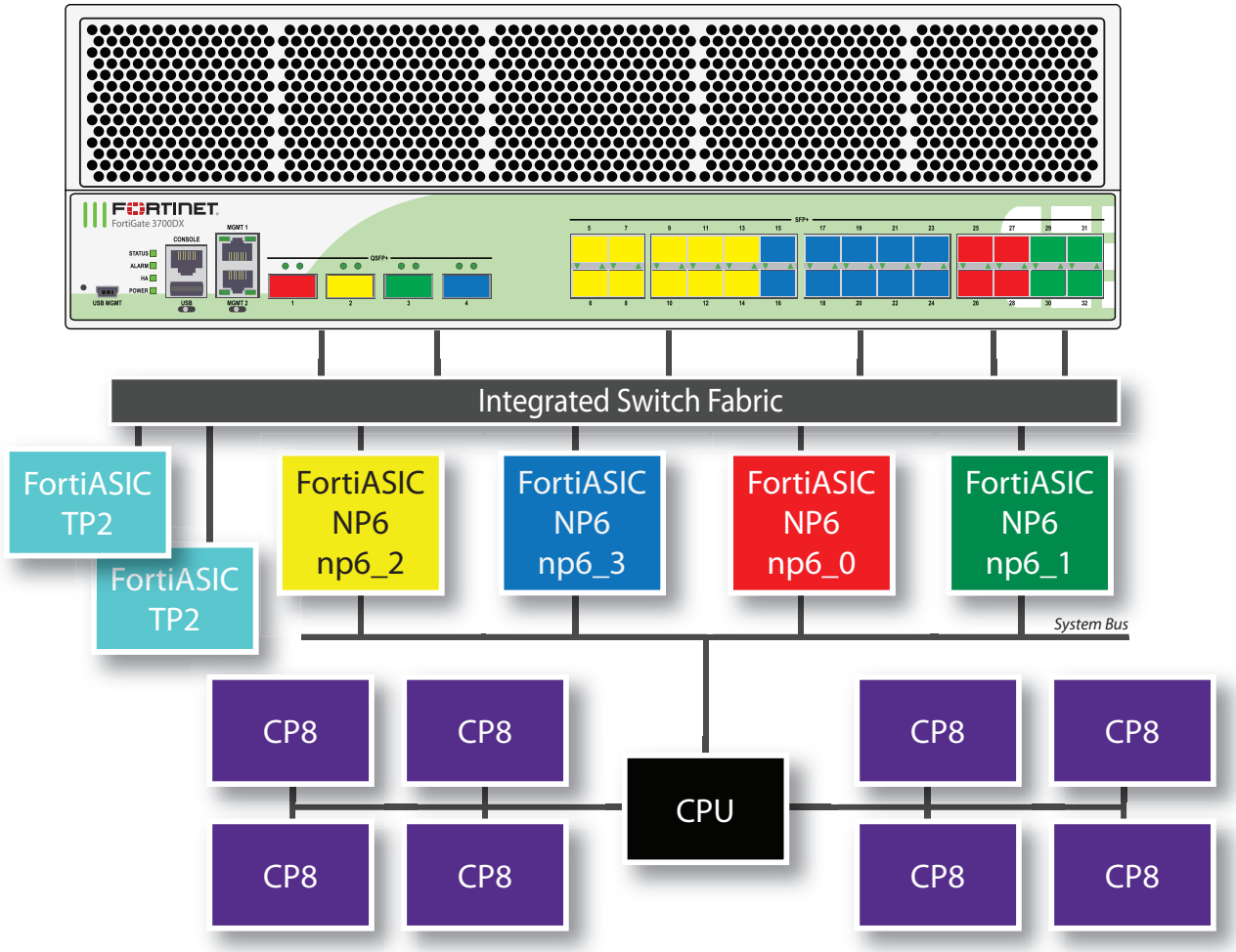
```
config system np6
   edit np6_0
      set low-latency-mode disable
   next
   edit np6_1
      set low-latency-mode disable
```

```
end
```

You do not have to turn off low latency to both np6_0 and np6_1. If you turn off low latency to just one NP6, the other NP6 will still be mapped according to the normal configuration.

In addition to turning off low latency, entering these commands also changes how ports are mapped to NP6s. Port1 is now mapped to np6_0 and port 3 is not mapped to np6_1. The FortiGate-3700DX has the following fastpath architecture:

- One 40Gb QSFP interface, port1, and four SFP+ 10Gb interfaces, port25 to port28 share connections to the first NP6 processor (np6_0).
- One 40Gb QSFP interface, port3, and four SFP+ 10Gb interfaces, port29 to port32 share connections to the second NP6 processor (np6_1).
- One 40Gb QSFP interface, port2 and ten SFP+ 10Gb interfaces, port5 to port14 share connections to the third NP6 processor (np6_2).
- One 40Gb QSFP interface, port4, and ten SFP+ 10Gb interfaces, port15 to port24 share connections to the fourth NP6 processor (np6_3).

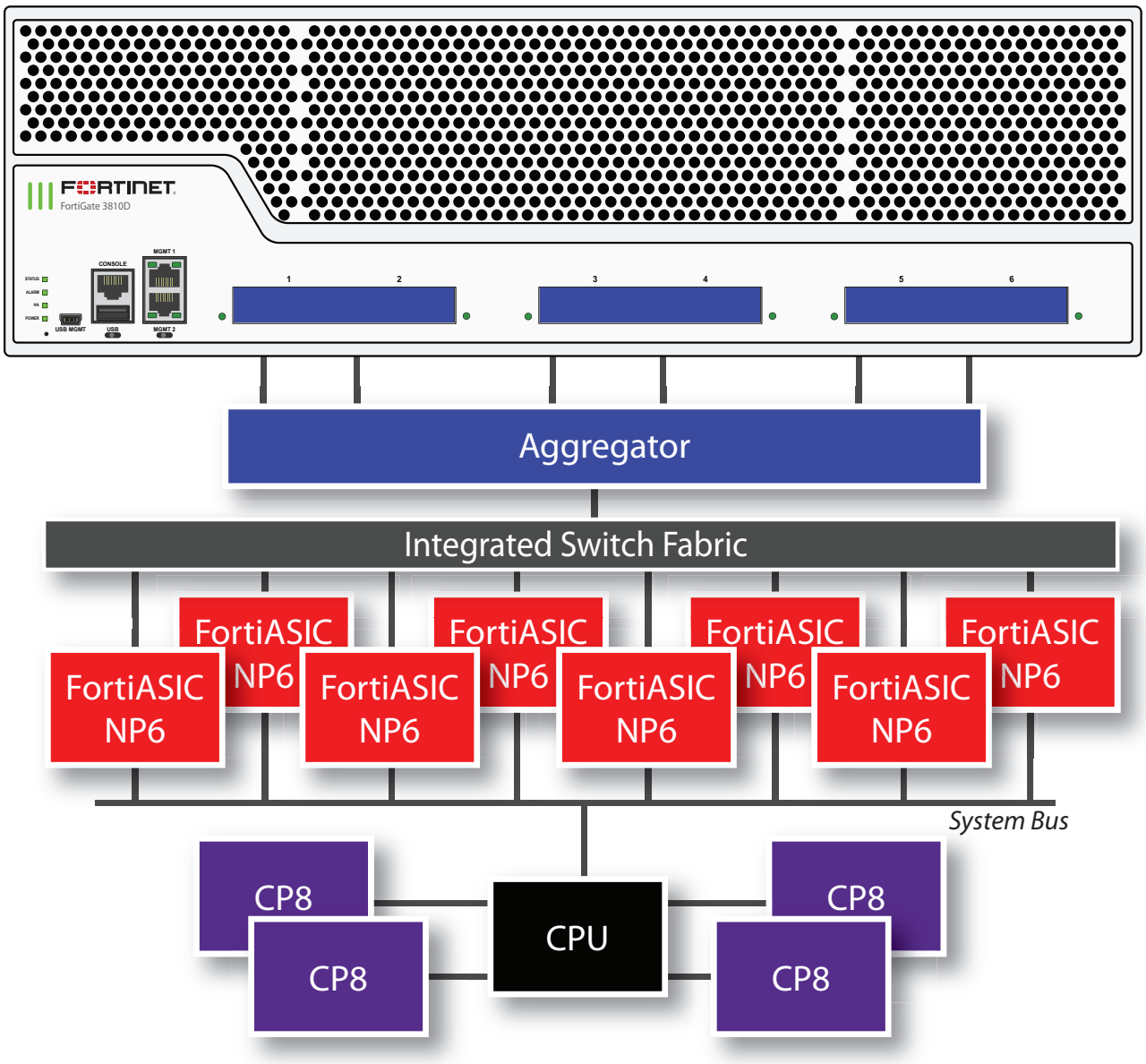


You can use the following diagnose command to display the FortiGate-3700DX NP6 configuration with low latency turned off for np6_0 and np6_1. The command output shows four NP6s named NP6_0, NP6_1, NP6_2, and NP6_3 and the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip   XAUI Ports            Max   Cross-chip
                             Speed offloading
------ ---- -------          ----- ----------
np6_0  0    port26           10G   Yes
       1    port25           10G   Yes
       2    port28           10G   Yes
       3    port27           10G   Yes
       0-3  port1            40G   Yes
------ ---- -------          ----- ----------
np6_1  0    port30           10G   Yes
       1    port29           10G   Yes
       2    port32           10G   Yes
       3    port31           10G   Yes
       0-3  port3            40G   Yes
------ ---- -------          ----- ----------
np6_2  0    port5            10G   Yes
       0    port9            10G   Yes
       0    port13           10G   Yes
       1    port6            10G   Yes
       1    port10           10G   Yes
       1    port14           10G   Yes
       2    port7            10G   Yes
       2    port11           10G   Yes
       3    port8            10G   Yes
       3    port12           10G   Yes
       0-3  port2            40G   Yes
------ ---- -------          ----- ----------
np6_3  0    port15           10G   Yes
       0    port19           10G   Yes
       0    port23           10G   Yes
       1    port16           10G   Yes
       1    port20           10G   Yes
       1    port24           10G   Yes
       2    port17           10G   Yes
       2    port21           10G   Yes
       3    port18           10G   Yes
       3    port22           10G   Yes
       0-3  port4            40G   Yes
------ ---- -------          ----- ----------
```

FortiGate-3810D fast path architecture

The FortiGate-3810D features six front panel 100Gigabit interfaces and eight NP6 processors connected to an Integrated Switch Fabric (ISF). Individual interfaces are not mapped to NP6 processors. Instead an Aggregator connects the front panel interfaces to the ISF. Because of the aggregator, no special mapping is required for fastpath offloading.

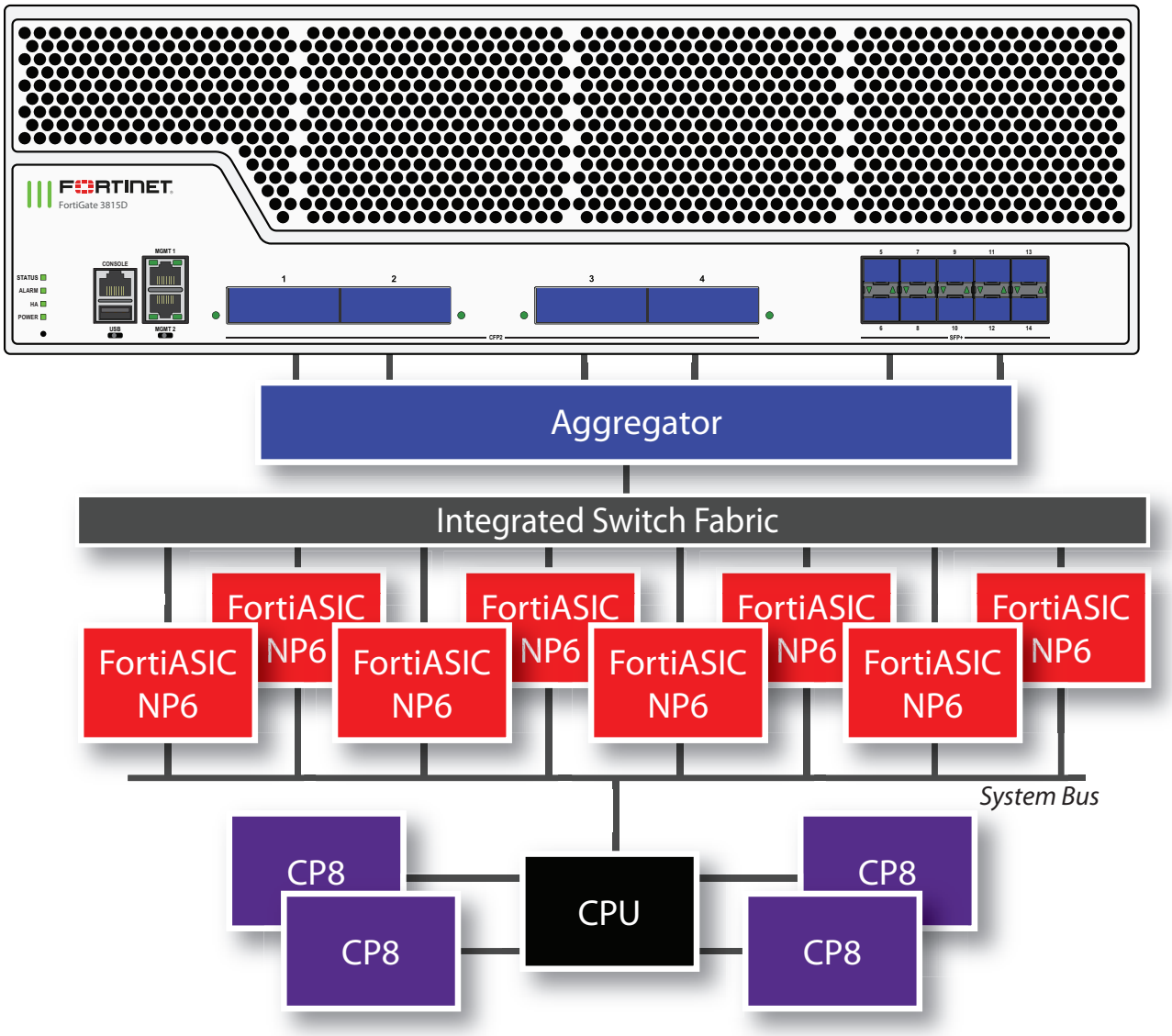


You can use the following diagnose command to display the FortiGate-3810D NP6 configuration. The command output shows all NP6s connected to each interface (port) with cross-chip offloading supported for each port.

```
diagnose npu np6 port-list
Chip    XAUI Ports   Max      Cross-chip
                     Speed    offloading
------ ---- ------- ------   ----------
all     0-3  port1   100000M Yes
all     0-3  port2   100000M Yes
all     0-3  port3   100000M Yes
all     0-3  port4   100000M Yes
all     0-3  port5   100000M Yes
all     0-3  port6   100000M Yes
------ ---- ------- ------   ----------
```

FortiGate-3815D fast path architecture

The FortiGate-3815D features four front panel 100Gigabit interfaces (port1 to port 4) and ten front panel 10Gigabit interfaces (port5 to port14) and eight NP6 processors connected to an Integrated Switch Fabric (ISF). Individual interfaces are not mapped to NP6 processors. Instead an Aggregator connects the front panel interfaces to the ISF. Because of the aggregator, no special mapping is required for fastpath offloading.



You can use the following diagnose command to display the FortiGate-3815D NP6 configuration. The command output shows all NP6s connected to each interface (port) with cross-chip offloading supported for each port.

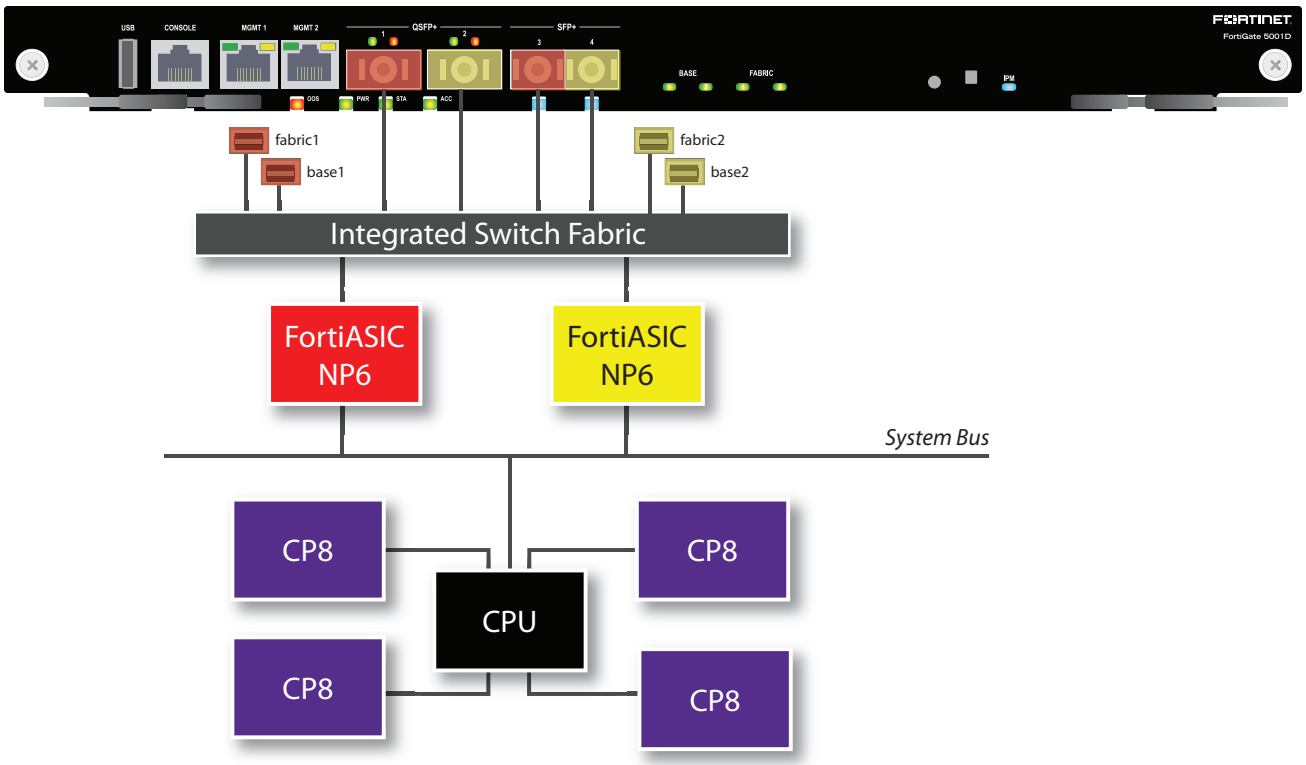
```
diagnose npu np6 port-list
Chip   XAUI Ports   Max      Cross-chip
                    Speed    offloading
------ ---- ------- ------   ----------
```

```
all     0-3  port1   100000M Yes
all     0-3  port2   100000M Yes
all     0-3  port3   100000M Yes
all     0-3  port4   100000M Yes
all     0-3  port11  10000M  Yes
all     0-3  port12  10000M  Yes
all     0-3  port13  10000M  Yes
all     0-3  port14  10000M  Yes
all     0-3  port10  10000M  Yes
all     0-3  port9   10000M  Yes
all     0-3  port8   10000M  Yes
all     0-3  port7   10000M  Yes
all     0-3  port5   10000M  Yes
all     0-3  port6   10000M  Yes
```

FortiGate-5001D fast path architecture

The FortiGate5001D features two NP6 processors.

- port1, port3, fabric1 and base1 share connections to the first NP6 processor.
- port2, port4, fabric2 and base2 share connections to the second NP6 processor.



NP6 default interface mapping

You can use the following command to display the FortiGate-5001D NP6 configuration. The command output shows two NP6s named NP6_0 and NP6_1. The output also shows the interfaces (ports) connected to each NP6.

```
diagnose npu np6 port-list
Chip   XAUI Ports            Max   Cross-chip
                            Speed offloading
------ ---- -------          ----- ----------

np6_0  0    port3            10G   Yes
       1
       2    base1            1G    Yes
       3
       0-3  port1            40G   Yes
       0-3  fabric1          40G   Yes
       0-3  fabric3          40G   Yes
       0-3  fabric5          40G   Yes
------ ---- -------          ----- ----------
np6_1  0
       1    port4            10G   Yes
       2
       3    base2            1G    Yes
       0-3  port2            40G   Yes
       0-3  fabric2          40G   Yes
       0-3  fabric4          40G   Yes
------ ---- -------          ----- ----------
```

NP6 interface mapping with split ports

If you use the following CLI command to split port1:

```
config system global
   set split-port port1
end
```

The new split ports (port1/1 to port 1/4) are mapped to the same NP6 as the un-split port1 interface:

```
diagnose npu np6 port-list
Chip   XAUI Ports            Max   Cross-chip
                            Speed offloading
------ ---- -------          ----- ----------
np6_0  0    port3            10G   Yes
       0    port1/1          10G   Yes
       1    port1/2          10G   Yes
       2    base1            1G    Yes
       2    port1/3          10G   Yes
       3    port1/4          10G   Yes
       0-3  fabric1          40G   Yes
       0-3  fabric3          40G   Yes
       0-3  fabric5          40G   Yes
------ ---- -------          ----- ----------
np6_1  0
       1    port4            10G   Yes
       2
       3    base2            1G    Yes
       0-3  port2            40G   Yes
       0-3  fabric2          40G   Yes
       0-3  fabric4          40G   Yes
------ ---- -------          ----- ----------
```

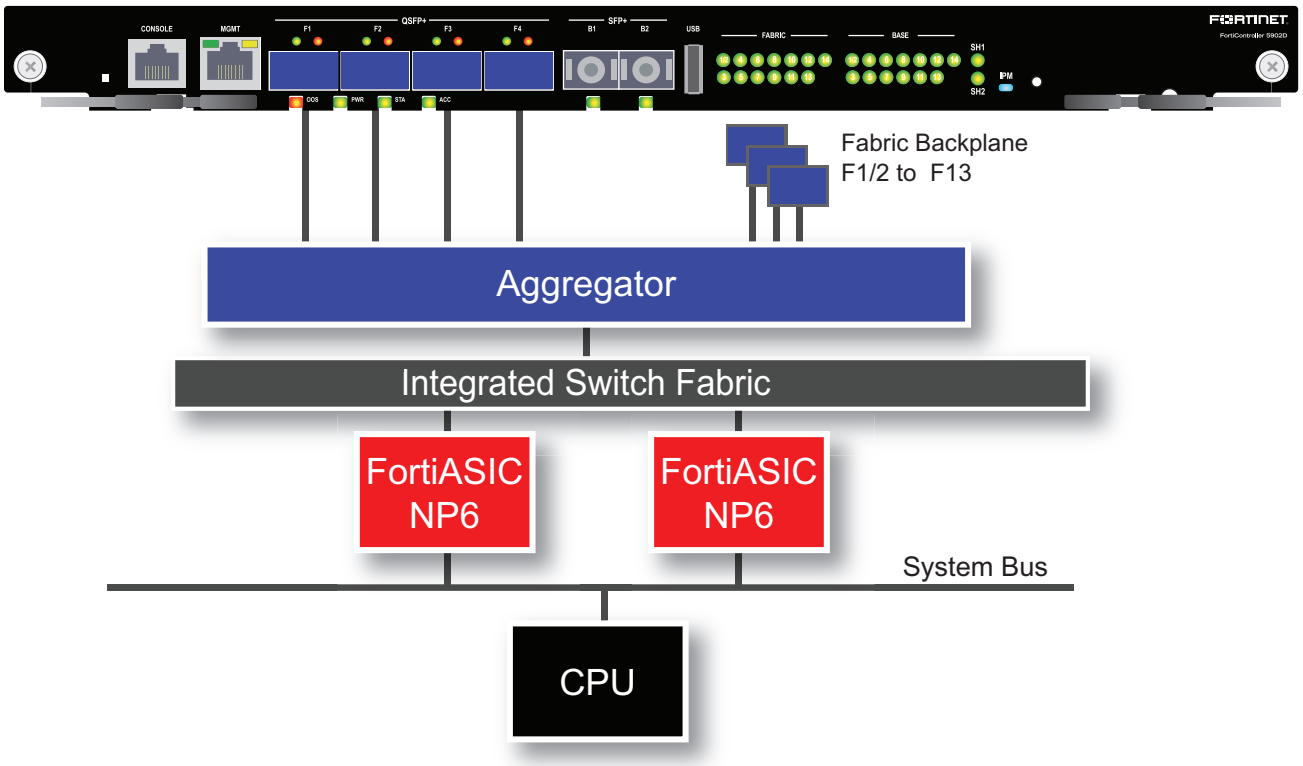
FortiController-5902D fast path architecture

The FortiController-5902D NP6 network processors and integrated switch fabric (ISF) provide hardware acceleration by offloading load balancing from the primary FortiController-5902D CPU. Network processors are especially useful for accelerating load balancing of TCP and UDP sessions.

The first packet of every new session is received by the primary FortiController-5902D and the primary FortiController-5902D uses its load balancing schedule to select the worker that will process the new session. This information is passed back to an NP6 network processor and all subsequent packets of the same sessions are offloaded to an NP6 network processor which sends the packet directly to a subordinate unit. Load balancing is effectively offloaded from the primary unit to the NP6 network processors resulting in a faster and more stable active-active cluster.

Traffic accepted by the FortiController-5902D F1 to F4 interfaces is that is processed by the primary FortiController-5902D is also be offloaded to the NP6 processors.

Individual FortiController-5902D interfaces are not mapped to NP6 processors. Instead an Aggregator connects the all fabric interfaces to the ISF and no special mapping is required for fastpath offloading.



NP6 content clustering mode interface mapping

FortiController-5902Ds run in content clustering mode and load balance sessions to FortiGate-5001D workers. Use the following command to enable content clustering:

```
config system elbc
   set mode content-cluster
   set inter-chassis-support enable
end
```

You can use the following command to display the content clustering FortiController-5902D NP6 configuration. The output shows that all ports are mapped to all NP6 processors.

```
diagose npu np6 port-list

Chip   XAUI Ports          Max     Cross-chip
                           Speed   offloading
------ ---- ----------     ------  ----------
all    0-3  f1             40000M  Yes
all    0-3  f2             40000M  Yes
all    0-3  f3             40000M  Yes
all    0-3  f4             40000M  Yes
all    0-3  np6_0_4        10000M  Yes
all    0-3  np6_0_5        10000M  Yes
all    0-3  elbc-ctrl/1-2  40000M  Yes
all    0-3  elbc-ctrl/3    40000M  Yes
all    0-3  elbc-ctrl/4    40000M  Yes
all    0-3  elbc-ctrl/5    40000M  Yes
all    0-3  elbc-ctrl/6    40000M  Yes
all    0-3  elbc-ctrl/7    40000M  Yes
all    0-3  elbc-ctrl/8    40000M  Yes
all    0-3  elbc-ctrl/9    40000M  Yes
all    0-3  elbc-ctrl/10   40000M  Yes
all    0-3  elbc-ctrl/11   40000M  Yes
all    0-3  elbc-ctrl/12   40000M  Yes
all    0-3  elbc-ctrl/13   40000M  Yes
all    0-3  elbc-ctrl/14   40000M  Yes
------ ---- ----------     ------  ----------
```

NP6 default interface mapping

You can use the following command to display the default FortiController-5902D NP6 configuration.

```
diagnose npu np6 port-list

Chip   XAUI Ports       Max     Cross-chip
                        Speed   offloading
------ ---- ----------  ------  ----------
all    0-3  f1          40000M  Yes
all    0-3  f2          40000M  Yes
all    0-3  f3          40000M  Yes
all    0-3  f4          40000M  Yes
all    0-3  np6_0_4     10000M  Yes
all    0-3  np6_0_5     10000M  Yes
all    0-3  fabric1/2   40000M  Yes
all    0-3  fabric3     40000M  Yes
all    0-3  fabric4     40000M  Yes
```

```
all    0-3  fabric5     40000M  Yes
all    0-3  fabric6     40000M  Yes
all    0-3  fabric7     40000M  Yes
all    0-3  fabric8     40000M  Yes
all    0-3  fabric9     40000M  Yes
all    0-3  fabric10    40000M  Yes
all    0-3  fabric11    40000M  Yes
all    0-3  fabric12    40000M  Yes
all    0-3  fabric13    40000M  Yes
all    0-3  fabric14    40000M  Yes
```

NP4 Acceleration

NP4 network processors provide fastpath acceleration by offloading communication sessions from the FortiGate CPU. When the first packet of a new session is received by an interface connected to an NP4 processor, just like any session connecting with any FortiGate interface, the session is forwarded to the FortiGate CPU where it is matched with a security policy. If the session is accepted by a security policy and if the session can be offloaded its session key is copied to the NP4 processor that received the packet. All of the rest of the packets in the session are intercepted by the NP4 processor and fast-pathed out of the FortiGate unit to their destination without ever passing through the FortiGate CPU. The result is enhanced network performance provided by the NP4 processor plus the network processing load is removed from the CPU. In addition, the NP4 processor can handle some CPU intensive tasks, like IPsec VPN encryption/decryption.

Session keys (and IPsec SA keys) are stored in the memory of the NP4 processor that is connected to the interface that received the packet that started the session. All sessions are fast-pathed and accelerated, even if they exit the FortiGate unit through an interface connected to another NP4. The key to making this possible is the Integrated Switch Fabric (ISF) that connects the NP4s and the FortiGate unit interfaces together. The ISF allows any port connectivity. All ports and NP4s can communicate with each other over the ISF.

There are no special ingress and egress fast path requirements because traffic enters and exits on interfaces connected to the same ISF. Most FortiGate models with multiple NP4 processors connect all interfaces and NP4 processors to the same ISF (except management interfaces) so this should not ever be a problem.

There is one limitation to keep in mind; the capacity of each NP4 processor. An individual NP4 processor has a capacity of 20 Gbps (10 Gbps ingress and 10 Gbps egress). Once an NP4 processor hits its limit, sessions that are over the limit are sent to the CPU. You can avoid this problem by as much as possible distributing incoming sessions evenly among the NP4 processors. To be able to do this you need to be aware of which interfaces connect to which NP4 processors and distribute incoming traffic accordingly.

Some FortiGate units contain one NP4 processor with all interfaces connected to it and to the ISF. As a result, offloading is supported for traffic between any pair of interfaces.

Some FortiGate units include NP4Lite processors. These network processors have the same functionality and limitations as NP4 processors but with about half the performance. NP4lite processors can be found in mid-range FortiGate models such as the FortiGate-200D and 240D.

Viewing your FortiGate's NP4 configuration

To list the NP4 network processors on your FortiGate unit, use the following CLI command.

```
get hardware npu np4 list
```

The output lists the interfaces that have NP4 processors. For example, for a FortiGate-5001C:

```
get hardware npu np4 list
ID    Model         Slot       Interface
0     On-board                 port1 port2 port3 port4
                               fabric1 base1 npu0-vlink0 npu0-vlink1
1     On-board                 port5 port6 port7 port8
                               fabric2 base2 npu1-vlink0 npu1-vlink1
```

NP4lite CLI commands (disabling NP4Lite offloading)

If your FortiGate unit includes an NP4Lite processor the following commands will be available:

- Use the following command to disable or enable NP4Lite offloading. By default NP4lite offloading is enabled. If you want to disable NP4Lite offloading to diagnose a problem enter:

```
diagnose npu nplite fastpath disable
```

This command disables NP4Lite offloading until your FortiGate reboots. You can also re-enable offloading by entering the following command:

```
diagnose npu nplite fastpath enable
```

- NP4lite debug command. Use the following command to debug NP4Lite operation:

```
diagnose npl npl_debug {<parameters>}
```

Configuring NP4 traffic offloading

Offloading traffic to a network processor requires that the FortiGate unit configuration and the traffic itself is suited to hardware acceleration. There are requirements for path the sessions and the individual packets.

NP4 session fast path requirements

Sessions must be fast path ready. Fast path ready session characteristics are:

- Layer 2 type/length must be 0x0800 (IEEE 802.1q VLAN specification is supported)
- Layer 3 protocol must be IPv4
- Layer 4 protocol must be UDP, TCP or ICMP
- Layer 3 / Layer 4 header or content modification must not require a session helper (for example, SNAT, DNAT, and TTL reduction are supported, but application layer content modification is not supported)
- Firewall policies must not include proxy-based security features (proxy-based virus scanning, proxy-based web filtering, DNS filtering, DLP, email filtering, VoIP, ICAP, or Proxy options).
- If the FortiGate supports NTurbo, firewall policies can include flow-based security features (IPS, Application Control, flow-based antivirus, or flow-based web filtering) .
- Origin must not be local host (the FortiGate unit)

If you disable anomaly checks by Intrusion Prevention (IPS), you can still enable NP4 hardware accelerated anomaly checks using the `fp-anomaly` field of the `config system interface` CLI command. See Offloading NP4 anomaly detection on page 1234Offloading NP4 anomaly detection on page 1234

If a session is not fast path ready, the FortiGate unit will not send the session key to the network processor(s). Without the session key, all session key lookup by a network processor for incoming packets of that session fails, causing all session packets to be sent to the FortiGate unit's main processing resources, and processed at normal speeds.

If a session is fast path ready, the FortiGate unit will send the session key to the network processor(s). Session key lookup then succeeds for subsequent packets from the known session.

Packet fast path requirements

Packets within the session must then also meet packet requirements.

- Incoming packets must not be fragmented.

- Outgoing packets must not require fragmentation to a size less than 385 bytes. Because of this requirement, the configured MTU (Maximum Transmission Unit) for network processors' network interfaces must also meet or exceed the network processors' supported minimum MTU of 385 bytes.

If packet requirements are not met, an individual packet will use FortiGate unit main processing resources, regardless of whether other packets in the session are offloaded to the specialized network processor(s).

In some cases, due to these requirements, a protocol's session(s) may receive a mixture of offloaded and non-offloaded processing.

For example, FTP uses two connections: a control connection and a data connection. The control connection requires a session helper, and cannot be offloaded, but the data connection does not require a session helper, and can be offloaded. Within the offloadable data session, fragmented packets will not be offloaded, but other packets will be offloaded.

Some traffic types differ from general offloading requirements, but still utilize some of the network processors' encryption and other capabilities. Exceptions include IPsec traffic and active-active high availability (HA) load balanced traffic.

Mixing fast path and non-fast path traffic

If packet requirements are not met, an individual packet will be processed by the FortiGate CPU regardless of whether other packets in the session are offloaded to the NP4.

Also, in some cases, a protocol's session(s) may receive a mixture of offloaded and non-offloaded processing. For example, VoIP control packets may not be offloaded but VoIP data packets (voice packets) may be offloaded.

Increasing NP4 offloading capacity using link aggregation groups (LAGs)

NP4 processors can offload sessions received by interfaces in link aggregation groups (LAGs) (IEEE 802.3ad). A LAG combines more than one physical interface into a group that functions like a single interface with a higher capacity than a single physical interface. For example, you could use a LAG if you want to offload sessions on a 3 Gbps link by adding three 1Gbps interfaces to the same LAG.

All offloaded traffic types are supported by LAGs, including IPsec VPN traffic. Just like with normal interfaces, traffic accepted by a LAG is offloaded by the NP4 processor connected to the interfaces in the LAG that receive the traffic to be offloaded. If all interfaces in a LAG are connected to the same NP4 processor, traffic received by that LAG is offloaded by that NP4 processor. The amount of traffic that can be offloaded is limited by the capacity of the NP4 processor.

If a FortiGate has two or more NP4 processors connected by an integrated switch fabric (ISF), you can use LAGs to increase offloading by sharing the traffic load across multiple NP4 processors. You do this by adding physical interfaces connected to different NP4 processors to the same LAG.

Adding a second NP4 processor to a LAG effectively doubles the offloading capacity of the LAG. Adding a third further increases offloading. The actual increase in offloading capacity may not actually be doubled by adding a second NP4 or tripled by adding a thrid. Traffic and load conditions and other factors may limit the actual offloading result.

The increase in offloading capacity offered by LAGs and multiple NP4s is supported by the ISF that allows multiple NP4 processors to share session information. On models that have more than one NP4 and no ISF, if you attempt to add interfaces connected to different NP4 processors to a LAG the system displays an error message.

There are also a few limitations to LAG NP4 offloading support for IPsec VPN:

- IPsec VPN anti-replay protection cannot be used if IPSec is configured on a LAG that has interfaces connected to multiple NP4 processors.
- Using a LAG connected to multiple NP4 processors for decrypting incoming IPsec VPN traffic may cause some of the incoming traffic to be decrypted by the CPU. So this configuration is not recommended since not all decryption is offloaded. (Using a LAG connected to multiple NP4 processors for encrypting outgoing IPsec VPN traffic is supported with no limitations.)
- Because the encrypted traffic for one IPsec VPN tunnel has the same 5-tuple, the traffic from one tunnel can only can be balanced to one interface in a LAG. This limits the maximum throughput for one IPsec VPN tunnel in an NP4 LAG group to 1Gbps.

NP4 traffic shaping offloading

Accelerated Traffic shaping is supported with the following limitations.

- NP4 processors support policy-based traffic shaping. However, fast path traffic and traffic handled by the FortiGate CPU (slow path) are controlled separately, which means the policy setting on fast path does not consider the traffic on the slow path.
- The port based traffic policing as defined by the inbandwidth and outbandwidth CLI commands is not supported.
- DSCP configurations are supported.
- Per-IP traffic shaping is supported.
- QoS in general is not supported.

You can also use the traffic shaping features of the FortiGate unit's main processing resources by disabling NP4 offloding. See Disabling NP offloading for firewall policies on page 1165.

NP4 IPsec VPN offloading

NP4 processors improve IPsec tunnel performance by offloading IPsec encryption and decryption.

Requirements for hardware accelerated IPsec encryption or decryption are a modification of general offloading requirements. Differing characteristics are:

- Origin can be local host (the FortiGate unit)
- In Phase 1 configuration, Local Gateway IP must be specified as an IP address of a network interface for a port attached to a network processor
- SA must have been received by the network processor
- in Phase 2 configuration:
  - encryption algorithm must be DES, 3DES, AES-128, AES-192, AES-256, or null
  - authentication must be MD5, SHA1, or null
  - if encryption is null, authentication must not also be null
  - if replay detection is enabled, `enc-offload-antireplay` must also be `enable` in the CLI

If replay detection is enabled in the Phase 2 configuration, you can enable or disable IPsec encryption and decryption offloading from the CLI. Performance varies by those CLI options and the percentage of packets requiring encryption or decryption. For details, see NP4 IPsec VPN offloading on page 1225

To apply hardware accelerated encryption and decryption, the FortiGate unit's main processing resources must first perform Phase 1 negotiations to establish the security association (SA). The SA includes cryptographic

processing instructions required by the network processor, such as which encryption algorithms must be applied to the tunnel. After ISAKMP negotiations, the FortiGate unit's main processing resources send the SA to the network processor, enabling the network processor to apply the negotiated hardware accelerated encryption or decryption to tunnel traffic.

Possible accelerated cryptographic paths are:

- IPsec decryption offload
  - Ingress ESP packet > Offloaded decryption > Decrypted packet egress (fast path)
  - Ingress ESP packet > Offloaded decryption > Decrypted packet to FortiGate unit's main processing resources
- IPsec encryption offload
  - Ingress packet > Offloaded encryption > Encrypted (ESP) packet egress (fast path)
  - Packet from FortiGate unit's main processing resources > Offloaded encryption > Encrypted (ESP) packet egress

NP4 IPsec VPN offloading configuration example

Hardware accelerated IPsec processing, involving either partial or full offloading, can be achieved in either tunnel or interface mode IPsec configurations.

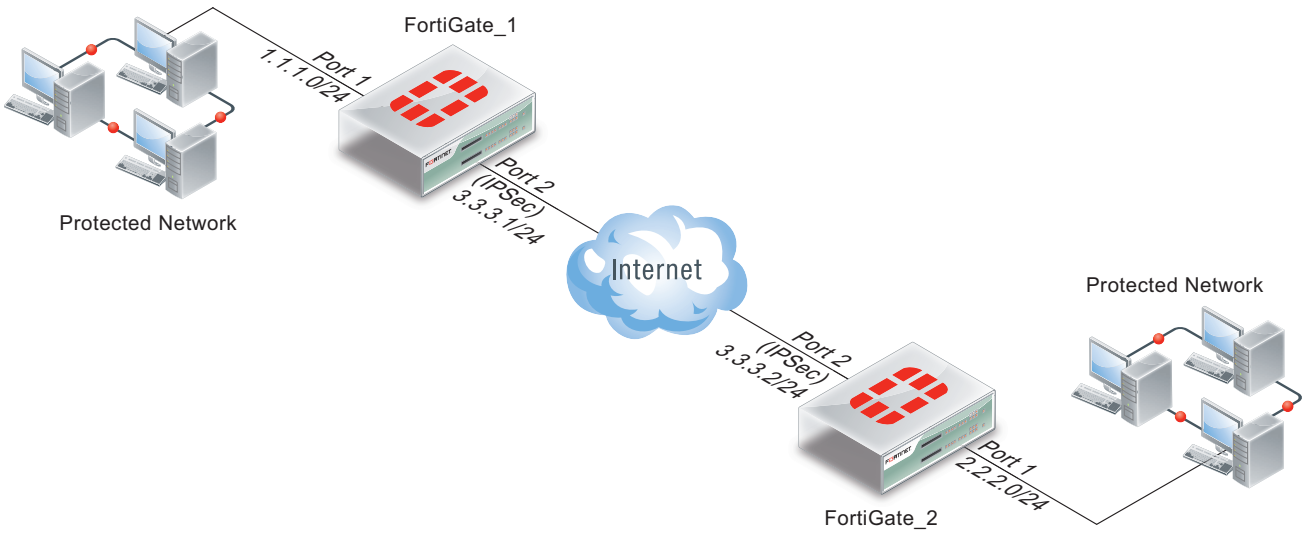
To achieve offloading for both encryption and decryption:

- In Phase 1 configuration's Advanced section, Local Gateway IP must be specified as an IP address of a network interface associated with a port attached to a network processor. (In other words, if Phase 1's Local Gateway IP is Main Interface IP, or is specified as an IP address that is not associated with a network interface associated with a port attached to a network processor, IPsec network processing is not offloaded.)
- In Phase 2 configuration's P2 Proposal section, if the checkbox "Enable replay detection" is enabled, `enc-offload-antireplay` and `dec-offload-antireplay` must be set to `enable` in the CLI.
- `offload-ipsec-host` must be set to `enable` in the CLI.

This section contains example IPsec configurations whose IPsec encryption and decryption processing is hardware accelerated by an NP4 unit contained in a FortiGate-5001B at both ends of the VPN tunnel.

Hardware accelerated IPsec VPN does not require both tunnel endpoints to have the same network processor model. However, if hardware is not symmetrical, the packet forwarding rate is limited by the slower side.

Example network topology for offloaded IPsec processing



Example ports and IP addresses for offloaded IPsec processing

	FortiGate_1		FortiGate_2	
	Port	**IP**	**Port**	**IP**
IPsec tunnel	FortiGate-5001B port 2	3.3.3.1/24	FortiGate-5001B port 2	3.3.3.2/24
Protected network	FortiGate-5001B port 1	1.1.1.0/24	FortiGate-5001B port 1	2.2.2.0/24

Accelerated policy mode IPsec configuration

The following steps create a hardware accelerated policy mode IPsec tunnel between two FortiGate-5001B units, each containing two NP4 processors, the first of which will be used.

To configure hardware accelerated policy mode IPsec

1. On FortiGate_1, go to **VPN > IPsec > Auto Key (IKE)**.
2. Configure Phase 1.
   For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.
   Select **Advanced**. In the Local Gateway IP section, select **Specify** and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2's FortiGate-ASM-FB4 module port 2.
3. Configure Phase 2.

4. Select **Enable replay detection**.
5. Use the following command to enable offloading antireplay packets:

```
config system npu
   set enc-offload-antireplay enable
end
```

   For details on encryption and decryption offloading options available in the CLI, see"Configuring NP accelerated VPN encryption/decryption offloading".

6. Go to **Policy > Policy > Policy**.
7. Configure a policy to apply the Phase 1 IPsec tunnel you configured in step 2 to traffic between FortiGate-5001B ports 1 and 2.
8. Go to **Router > Static > Static Route**.
9. Configure a static route to route traffic destined for FortiGate_2's protected network to VPN IP address of FortiGate_2's VPN gateway, 3.3.3.2, through the FortiGate-5001B port2.
   You can also configure the static route using the following CLI command:

```
config router static
   edit 2
      set device "AMC-SW1/2"
      set dst 2.2.2.0 255.255.255.0
      set gateway 3.3.3.2
   end
```

10. On FortiGate_2, go to **VPN > IPsec > Auto Key (IKE)**.
11. Configure Phase 1.
    For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.
    Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's port2.
12. Configure Phase 2.
13. Select **Enable replay detection**.
14. Use the following command to enable offloading antireplay packets:

```
config system npu
   set enc-offload-antireplay enable
end
```

    For details on encryption and decryption offloading options available in the CLI, see Configuring NP accelerated IPsec VPN encryption/decryption offloading on page 1163.

15. Go to **Policy > Policy > Policy**.
16. Configure a policy to apply the Phase 1 IPsec tunnel you configured in step 9 to traffic between FortiGate-5001B ports 1 and 2.
17. Go to **Router > Static > Static Route**.
18. Configure a static route to route traffic destined for FortiGate_1's protected network to VPN IP address of FortiGate_1's VPN gateway, 3.3.3.1, through the FortiGate-5001B port2.
    You can also configure the static route using the following CLI commands:

```
config router static
   edit 2
      set device "AMC-SW1/2"
      set dst 1.1.1.0 255.255.255.0
      set gateway 3.3.3.1
   end
```

19. Activate the IPsec tunnel by sending traffic between the two protected networks.
    To verify tunnel activation, go to **VPN > Monitor > IPsec Monitor**.

Accelerated interface mode IPsec configuration

The following steps create a hardware accelerated interface mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

To configure hardware accelerated interface mode IPsec

1. On FortiGate_1, go to **VPN > IPsec > Auto Key (IKE)**.
2. Configure Phase 1.
   For interface mode IPsec and for hardware acceleration, the following settings are required.
   - Select Advanced.
   - Enable the checkbox “Enable IPsec Interface Mode.”
   - In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2’s port 2.
3. Configure Phase 2.
4. Select **Enable replay detection**.
5. Use the following command to enable offloading antireplay packets:

```
config system npu
   set enc-offload-antireplay enable
end
```

   For details on encryption and decryption offloading options available in the CLI, see "Configuring NP accelerated VPN encryption/decryption offloading".

6. Go to **Policy > Policy > Policy**.
7. Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.
8. Go to **Router > Static > Static Route**.
9. Configure a static route to route traffic destined for FortiGate_2’s protected network to the Phase 1 IPsec device, `FGT_1_IPsec`.
   You can also configure the static route using the following CLI commands:

```
config router static
   edit 2
      set device "FGT_1_IPsec"
      set dst 2.2.2.0 255.255.255.0
   end
```

10. On FortiGate_2, go to **VPN > IPsec > Auto Key (IKE)**.
11. Configure Phase 1.
    For interface mode IPsec and for hardware acceleration, the following settings are required.
    - Enable the checkbox “Enable IPsec Interface Mode.”
    - In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1’s FortiGate-5001B port 2.
12. Configure Phase 2.
13. Select **Enable replay detection**.
14. Use the following command to enable offloading antireplay packets:

```
config system npu
```

```
    set enc-offload-antireplay enable
  end
```

For details on encryption and decryption offloading options available in the CLI, see " Hardware acceleration overview" on page 1155.

15. Go to **Policy > Policy > Policy**.
16. Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 9 to traffic leaving from or arriving on FortiGate-5001B port 1.
17. Go to **Router > Static > Static Route**.
18. Configure a static route to route traffic destined for FortiGate_1's protected network to the Phase 1 IPsec device, `FGT_2_IPsec`.
    You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_2_IPsec"
    set dst 1.1.1.0 255.255.255.0
    next
  end
```

19. Activate the IPsec tunnel by sending traffic between the two protected networks.
    To verify tunnel activation, go to **VPN > Monitor > IPsec Monitor**.

Configuring Inter-VDOM link acceleration with NP4 processors

FortiGate units with NP4 processors include inter-VDOM links that can be used to accelerate inter-VDOM link traffic.

Traffic is blocked if you enable IPS for traffic passing over inter-VDOM links if that traffic is being offloaded by an NP4 processor.If you disable NP4 offloading traffic will be allowed to flow. You can disable offloading in individual firewall policies by disabling `auto-asic-offload` for individual policies. You can also use the following command to disable all IPS offloading

```
config ips global
  set np-accel-mode {none | basic}
  set cp-accel-mode {none | basic | advanced}
end
```

- For a FortiGate unit with two NP4 processors there are also two inter-VDOM links, each with two interfaces:
  - **npu0-vlink:**
    npu0-vlink0
    npu0-vlink1
  - **npu1-vlink:**
    npu1-vlink0
    npu1-vlink1

These interfaces are visible from the GUI and CLI. For a FortiGate unit with NP4 interfaces, enter the following CLI command (output shown for a FortiGate-5001B):

```
get hardware npu np4 list
ID    Model         Slot       Interface
0     On-board                 port1 port2 port3 port4
                               fabric1 base1 npu0-vlink0 npu0-vlink1
1     On-board                 port5 port6 port7 port8
```

```
fabric2 base2 npu1-vlink0 npu1-vlink1
```

By default the interfaces in each inter-VDOM link are assigned to the root VDOM. To use these interfaces to accelerate inter-VDOM link traffic, assign each interface in a pair to the VDOMs that you want to offload traffic between. For example, if you have added a VDOM named New-VDOM to a FortiGate unit with NP4 processors, you can go to **System > Network > Interfaces** and edit the **npu0-vlink1** interface and set the **Virtual Domain** to **New-VDOM**.

This results in an inter-VDOM link between root and New-VDOM. You can also do this from the CLI:

```
config system interface
   edit npu0-vlink1
      set vdom New-VDOM
end
```

Using VLANs to add more accelerated Inter-VDOM links

You can add VLAN interfaces to the accelerated inter-VDOM links to create inter-VDOM links between more VDOMs. For the links to work, the VLAN interfaces must be added to the same inter-VDOM link, must be on the same subnet, and must have the same VLAN ID.

For example, to accelerate inter-VDOM link traffic between VDOMs named Marketing and Engineering using VLANs with VLAN ID 100 go to **System > Network > Interfaces** and select **Create New** to create the VLAN interface associated with the Marketing VDOM:

Name	Marketing-link
Type	VLAN
Interface	npu0-vlink0
VLAN ID	100
Virtual Domain	Marketing
IP/Network Mask	172.20.120.12/24

Create the inter-VDOM link associated with Engineering VDOM:

Name	Engineering-link
Type	VLAN
Interface	npu0-vlink1
VLAN ID	100
Virtual Domain	Engineering
IP/Network Mask	172.20.120.22/24

Or do the same from the CLI:

```
config system interface
   edit Marketing-link
      set vdom Marketing
      set ip 172.20.120.12/24
      set interface npu0-vlink0
      set vlanid 100
   next
   edit Engineering-link
      set vdom Engineering
      set ip 172.20.120.22/24
      set interface npu0-vlink1
      set vlanid 100
```

Confirm that the traffic is accelerated

Use the following CLI commands to obtain the interface index and then correlate them with the session entries. In the following example traffic was flowing between new accelerated inter-VDOM links and physical ports port1 and port 2 also attached to the NP4 processor.

```
diagnose ip address list
IP=172.31.17.76->172.31.17.76/255.255.252.0 index=5 devname=port1
IP=10.74.1.76->10.74.1.76/255.255.252.0 index=6 devname=port2
IP=172.20.120.12->172.20.120.12/255.255.255.0 index=55 devname=IVL-VLAN1_ROOT
IP=172.20.120.22->172.20.120.22/255.255.255.0 index=56 devname=IVL-VLAN1_VDOM1

diagnose sys session list
session info: proto=1 proto_state=00 duration=282 expire=24 timeout=0 session info:
    proto=1 proto_state=00 duration=124 expire=59 timeout=0 flags=00000000
    sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=180/3/1 reply=120/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=55->5/5->55
    gwy=172.31.19.254/172.20.120.22
hook=post dir=org act=snat 10.74.2.87:768->10.2.2.2:8(172.31.17.76:62464)
hook=pre dir=reply act=dnat 10.2.2.2:62464->172.31.17.76:0(10.74.2.87:768)
misc=0 policy_id=4 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=0000004e tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=10.74.2.87, bps=880
npu_state=00000000
npu info: flag=0x81/0x81, offload=4/4, ips_offload=0/0, epid=160/218, ipid=218/160,
    vlan=32769/0

session info: proto=1 proto_state=00 duration=124 expire=20 timeout=0 flags=00000000
    sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=180/3/1 reply=120/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=6->56/56->6
    gwy=172.20.120.12/10.74.2.87
hook=pre dir=org act=noop 10.74.2.87:768->10.2.2.2:8(0.0.0.0:0)
```

```
hook=post dir=reply act=noop 10.2.2.2:768->10.74.2.87:0(0.0.0.0:0)
misc=0 policy_id=3 id_policy_id=0 auth_info=0 chk_client_info=0 vd=1
serial=0000004d tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=10.74.2.87, bps=880
npu_state=00000000
npu info: flag=0x81/0x81, offload=4/4, ips_offload=0/0, epid=219/161, ipid=161/219,
    vlan=0/32769
total session 2
```

Offloading NP4 anomaly detection

Network interfaces associated with a port attached to an NP4 processor can be configured to offload anomaly checking to the NP4 processor. This anomaly checking happens before other offloading and separately from DoS policy anomaly checking. Using the following command, each FortiGate interface can have a different anomaly checking configuration even if they are connected to the same NP4 processor.

The options available for this command apply anomaly checking for NP4 sessions in the same way as the command descrbed in Configuring individual NP6 processors on page 1178 applies anomaly checking for for NP6 sessions.

```
config system interface
   edit <port-name>
      set fp-anomaly <anomalies>
   end
```

where `<anomalies>` can be one, more than one or all of the following:

Anomaly	Description
drop_icmp_frag	Drop ICMP fragments to pass.
drop_icmpland	Drop ICMP Land.
drop_ipland	Drop IP Land.
drop_iplsrr	Drop IP with Loose Source Record Route option.
drop_iprr	Drop IP with Record Route option.
drop_ipsecurity	Drop IP with Security option.
drop_ipssrr	Drop IP with Strict Source Record Route option.
drop_ipstream	Drop IP with Stream option.
drop_iptimestamp	Drop IP with Timestamp option.
drop_ipunknown_option	Drop IP with malformed option.
drop_ipunknown_prot	Drop IP with Unknown protocol.
drop_tcp_fin_noack	Drop TCP FIN with no ACT flag set to pass.
drop_tcp_no_flag	Drop TCP with no flag set to pass.
drop_tcpland	Drop TCP Land.
drop_udpland	Drop UDP Land.
drop_winnuke	Drop TCP WinNuke.
pass_icmp_frag	Allow ICMP fragments to pass.
pass_icmpland	Allow ICMP Land to pass.
pass_ipland	Allow IP land to pass.
pass_iplsrr	Allow IP with Loose Source Record Route option to pass.
pass_iprr	Allow IP with Record Route option to pass.
pass_ipsecurity	Allow IP with Security option to pass.
pass_ipssrr	Allow IP with Strict Source Record Route option to pass.

Anomaly	Description
pass_ipstream	Allow IP with Stream option to pass.
pass_iptimestamp	Allow IP with Timestamp option to pass.
pass_ipunknown_option	Allow IP with malformed option to pass.
pass_ipunknown_prot	Allow IP with Unknown protocol to pass.
pass_tcp_fin_noack	Allow TCP FIN with no ACT flag set to pass.
pass_tcp_no_flag	Allow TCP with no flag set to pass.
pass_tcpland	Allow TCP Land to pass.
pass_udpland	Allow UDP Land to pass.
pass_winnuke	Allow TCP WinNuke to pass.

Example

You might configure an NP4 to drop packets with TCP WinNuke or unknown IP protocol anomalies, but to pass packets with an IP time stamp, using hardware acceleration provided by the network processor.

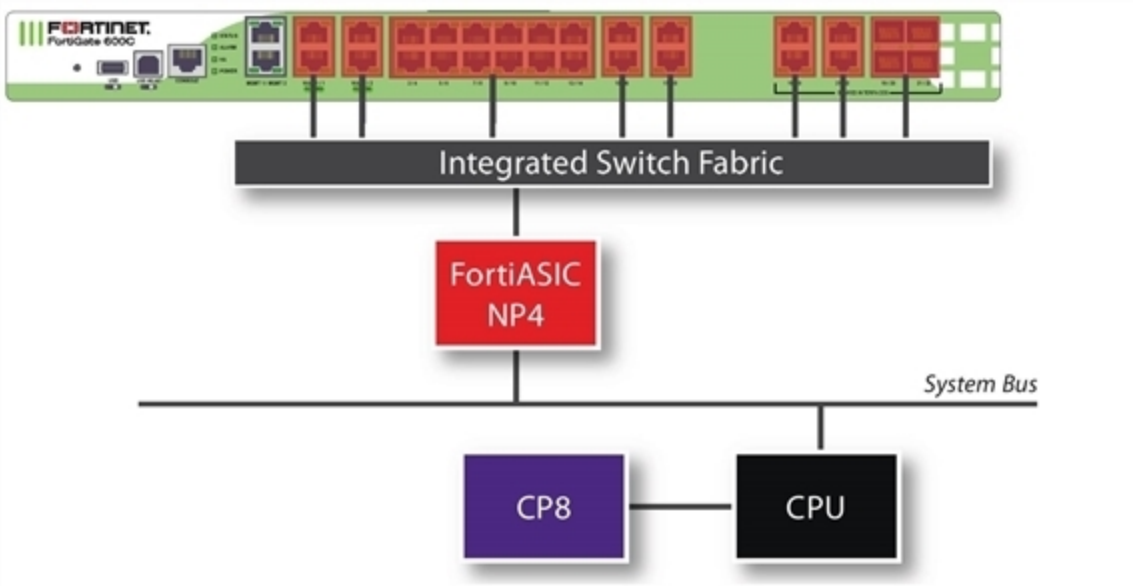
```
config system interface
   edit port1
      set fp-anomaly drop_winnuke drop_ipunknown_prot pass_iptimestamp
   end
```

FortiGate NP4 architectures

This chapter shows the NP4 architecture for the all FortiGate units and modules that include NP4 processors.

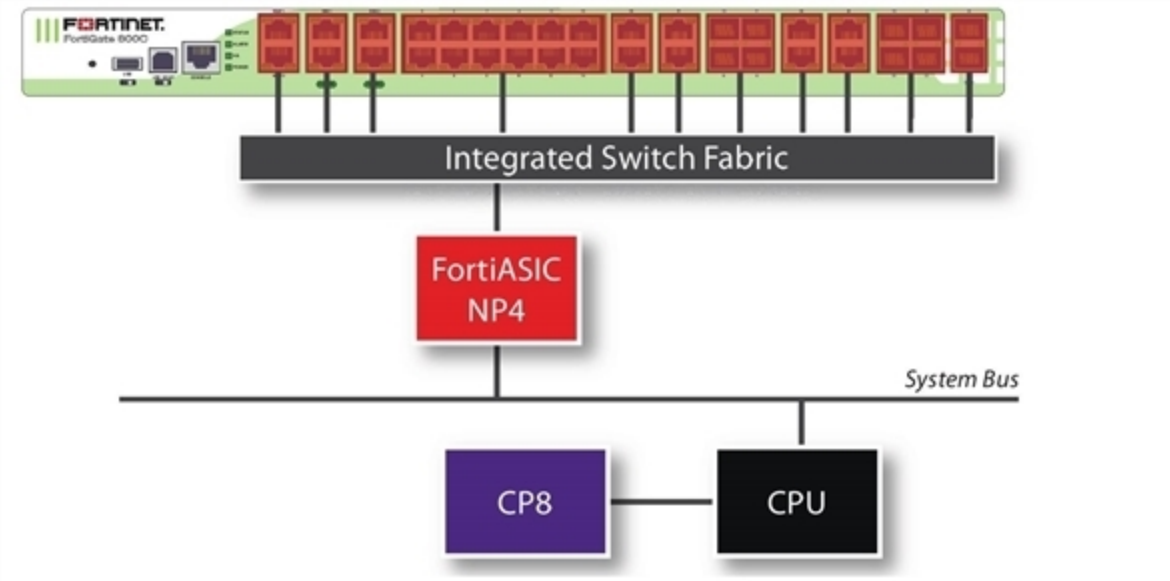
FortiGate-600C

The FortiGate-600C features one NP4 processor. All the ports are connected to this NP4 over the Integrated Switch Fabric. Port1 and port2 are dual failopen redundant RJ-45 ports. Port3-port22 are RJ-45 ethernet ports, and there are four 1Gb SFP interface ports duplicating the port19-port22 connections.



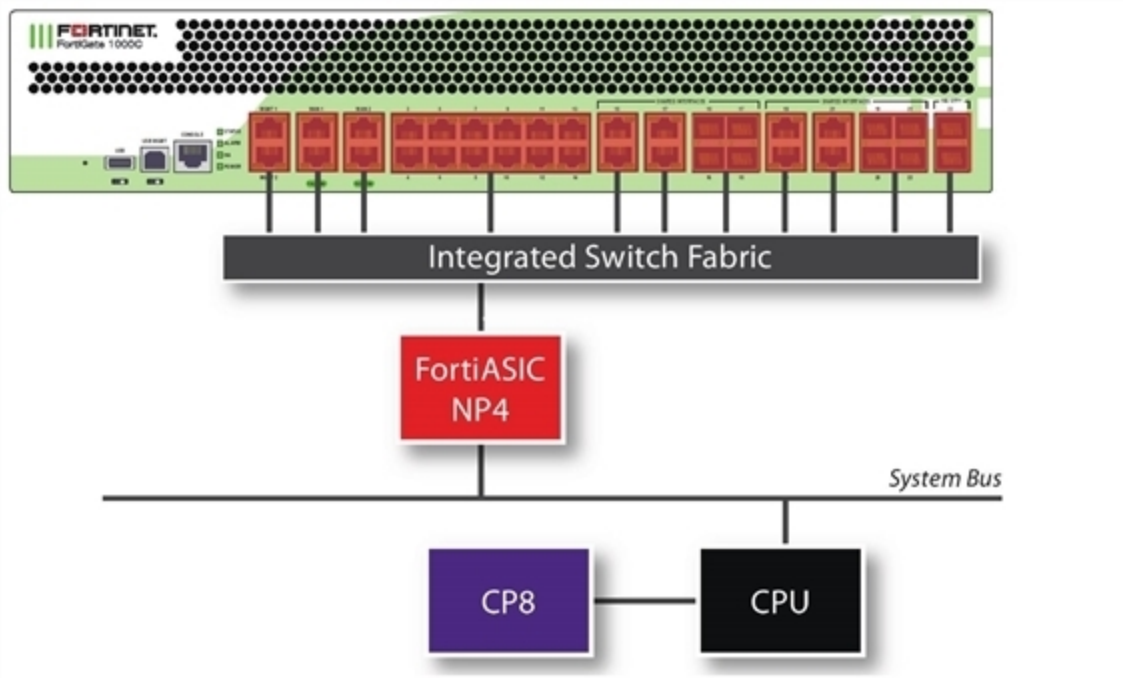
FortiGate-800C

The FortiGate-800C features one NP4 processor. All the ports are connected to this NP4. Port1 and port2 are dual failopen redundant RJ-45 ports. Port3-port22 are RJ-45 ethernet ports, and there are eight 1Gb SFP interface ports duplicating the port15-18 and port19-port22 connections. There are also two 10Gb SFP+ ports, port23 and port24.



FortiGate-1000C

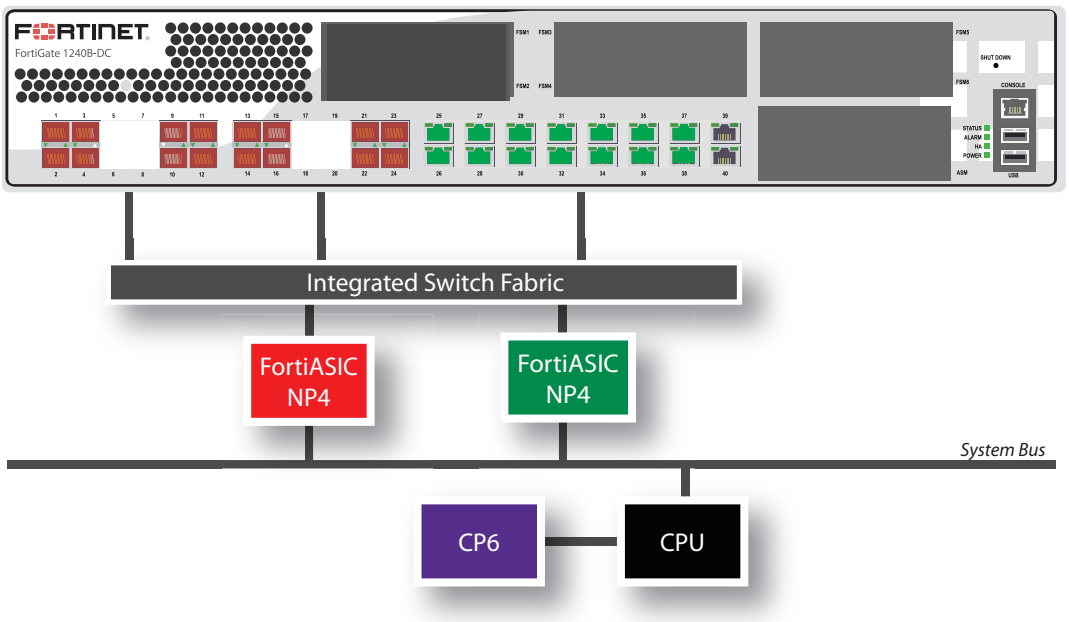
The FortiGate-1000C features one NP4 processor. All the ports are connected to this NP4. Port1 and port2 are dual failopen redundant RJ-45 ports. Port3-port22 are RJ-45 ethernet ports, and there are eight 1Gb SFP interface ports duplicating the port15-18 and port19-port22 connections. There are also two 10Gb SFP+ ports, port23 and port24.



FortiGate-1240B

The FortiGate-1240B features two NP4 processors:

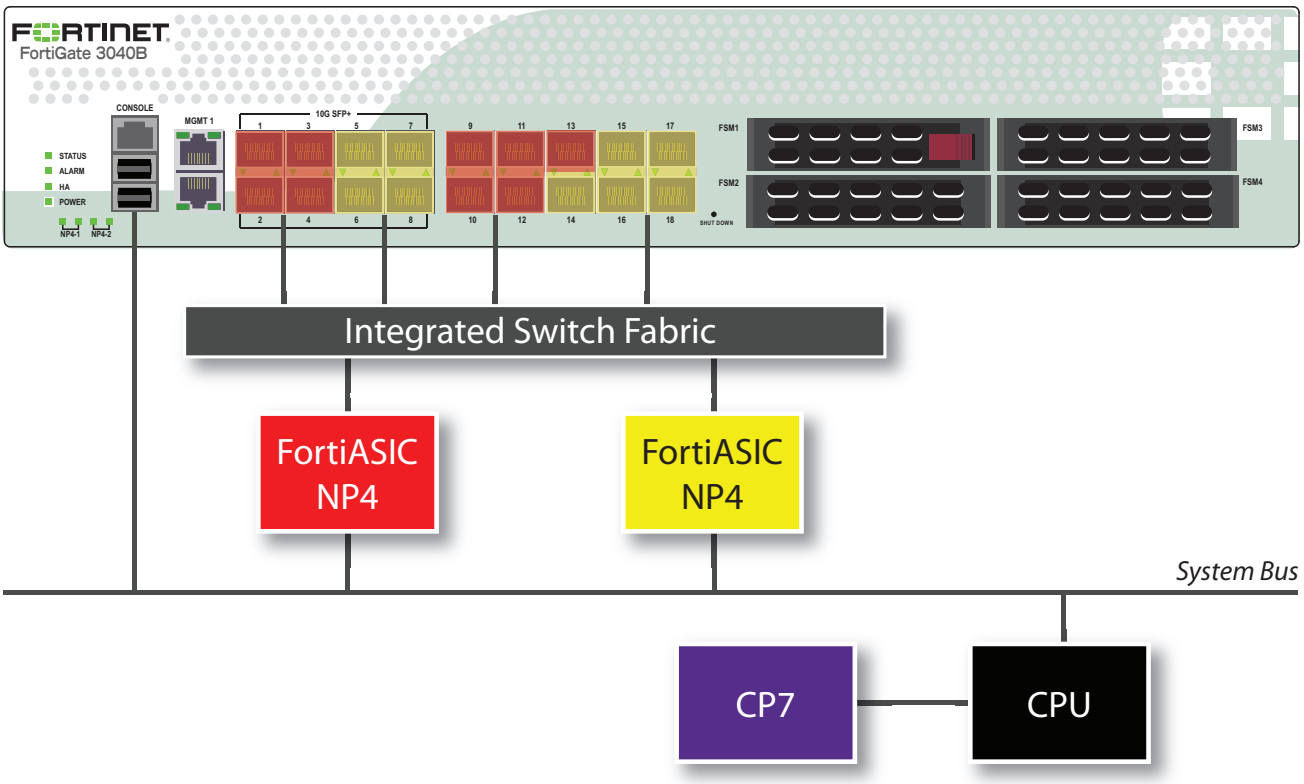
- Port1 to port24 are 1Gb SFP interfaces connected to one NP4 processor.
- Port25 to port38 are RJ-45 ethernet ports, connected to the other NP4 processor.
- Port39 and port40 are not connected to an NP4 processor.



FortiGate-3040B

The FortiGate-3040B features two NP4 processors:

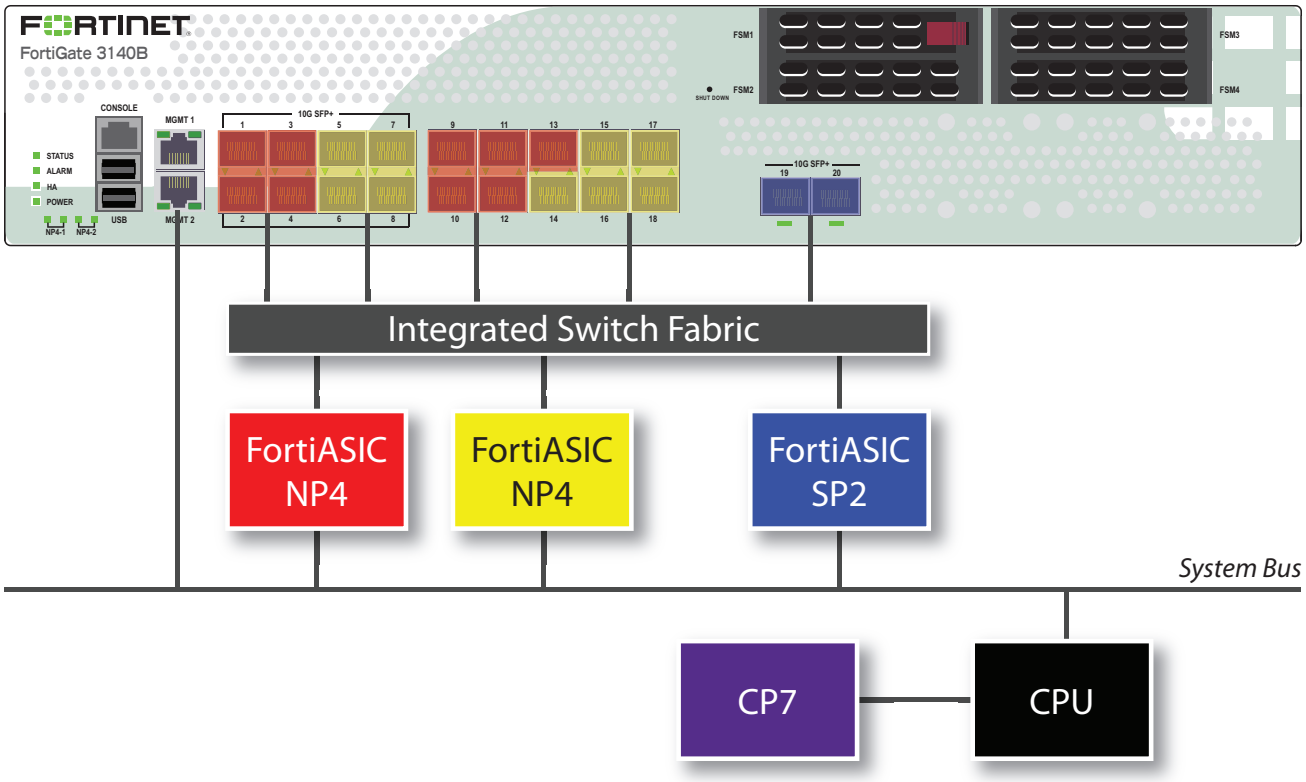
- The 10Gb interfaces, port1, port2, port3, port4, and the 1Gb interfaces, port9, port10, port11, port12, port13, share connections to one NP4 processor.
- The 10Gb interfaces, port5, port6, port7, port8, and the 1Gb interfaces, port14, port15, port16, port17, port18, share connections to the other NP4 processor.



FortiGate-3140B

The FortiGate-3140B features two NP4 processors and one SP2 processor:

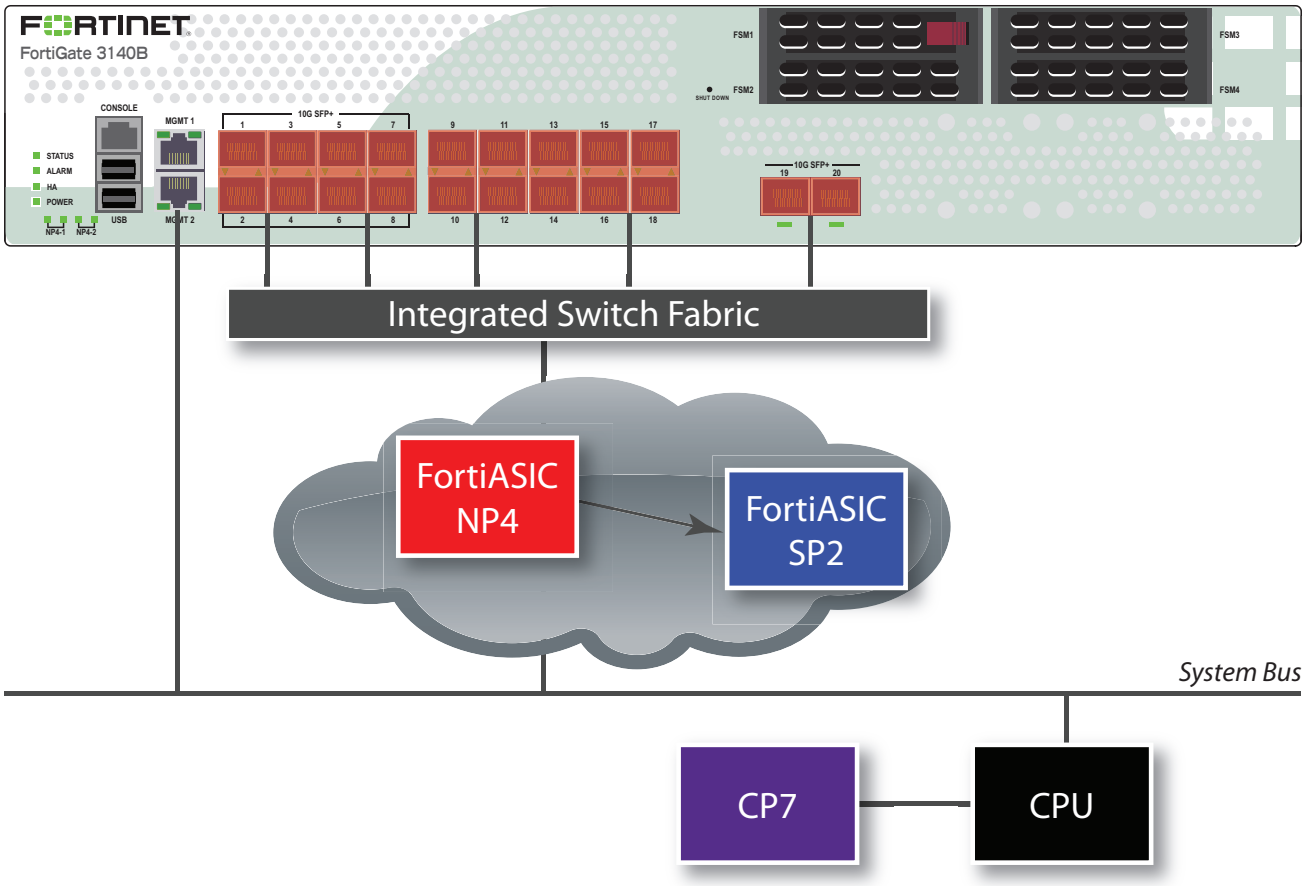
- The 10Gb interfaces, port1, port2, port3, port4, and the 1Gb interfaces, port9, port10, port11, port12, port13, share connections to one NP4 processor.
- The 10Gb interfaces, port5, port6, port7, port8, and the 1Gb interfaces, port14, port15, port16, port17, port18, share connections to the other NP4 processor.
- The 10Gb interfaces, port19 and port20, share connections to the SP2 processor.



FortiGate-3140B — load balance mode

The FortiGate-3140B load balance mode allows you increased flexibility in how you use the interfaces on the FortiGate unit. When enabled, traffic between any two interfaces (excluding management and console) is accelerated. Traffic is not limited to entering and leaving the FortiGate unit in specific interface groupings to benefit from NP4 and SP2 acceleration. You can use any pair of interfaces.

Security acceleration in this mode is limited, however. Only IPS scanning is accelerated in load balance mode.



To enable this feature, issue this CLI command.

```
config system global
   set sp-load-balance enable
end
```

The FortiGate unit will then restart.

To return to the default mode, issue this CLI command.

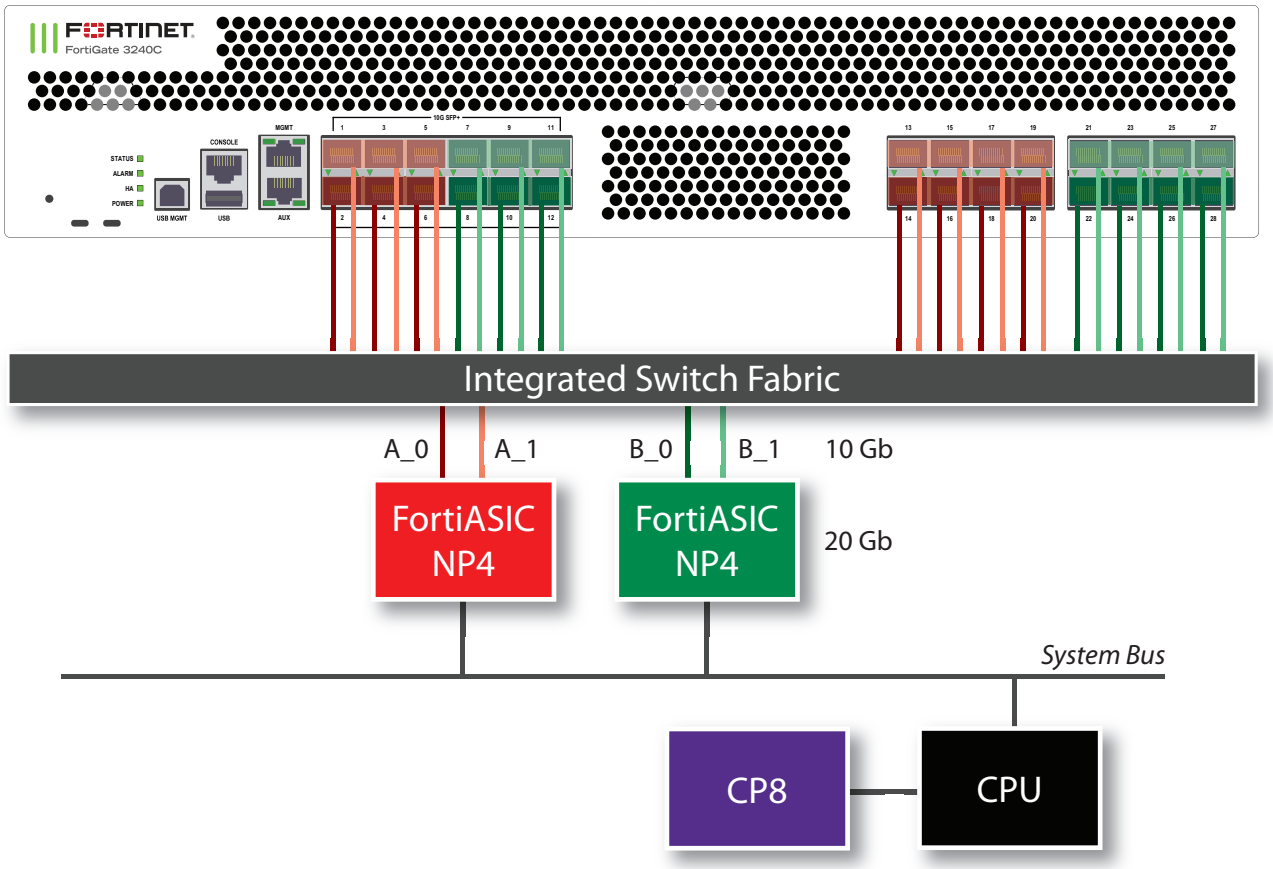
```
config system global
   set sp-load-balance disable
end
```

FortiGate-3240C

The FortiGate-3240C features two NP4 processors:

- The 10Gb interfaces, port1 through port6, and the 1Gb interfaces, port13 through port20, share connections to one NP4 processor.
- The 10Gb interfaces, port7 through port12, and the 1Gb interfaces, port21 through port28, share connections to the other NP4 processor.

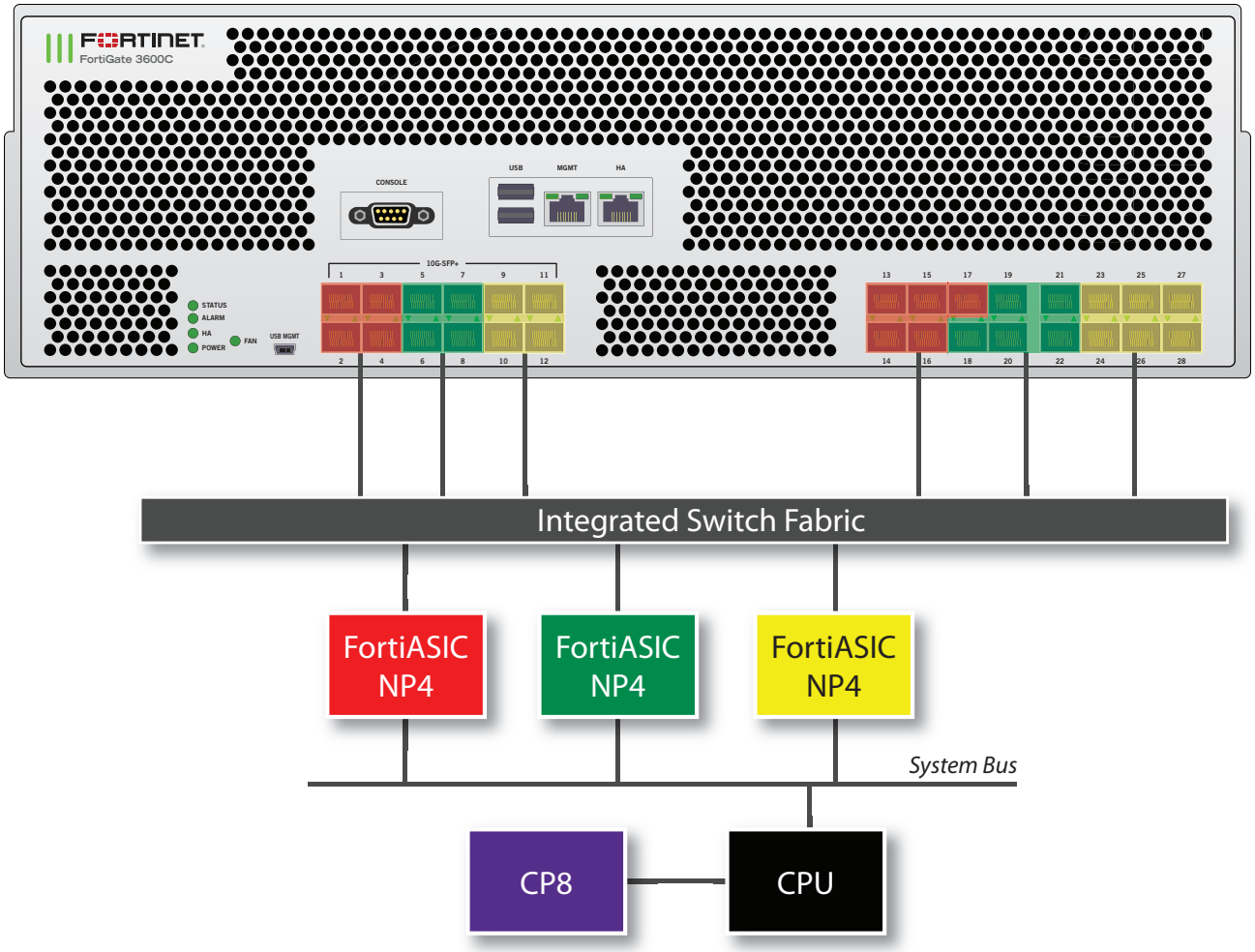
In addition to the ports being divided between the two NP4 processors, they are further divided between the two connections to each processor. Each NP4 can process 20 Gb of network traffic per second and each of two connections to each NP4 can move 10Gb of data to the processor per second, so the ideal configuration would have no more than 10 Gb of network traffic to each connection of each NP4 at any time.



FortiGate-3600C

The FortiGate-3600C features three NP4 processors:

- The 10Gb interfaces, port1-port4, and the 1Gb interfaces, port13-port17, share connections to one NP4 processor.
- The 10Gb interfaces, port5-port8, and the 1Gb interfaces, port18-port22 share connections to the second NP4 processor.
- The 10Gb interfaces, port9-port12, and the 1Gb interfaces, port23-port28 share connections to the third NP4 processor.



FortiGate-3600C XAUI interfaces

The FortiGate-3600C uses XAUI links for communication between physical Ethernet ports and the integrated switch fabric.

Each XAUI link has a maximum bandwidth of 10-Gigabits. The reason you may need to know about the XAUI link in NP4 configurations is because of this 10-Gigabit limit. Because of this limitation, the total amount of data processed by all Ethernet interfaces connected to an XAUI link cannot exceed 10 gigabits. In some cases this may limit the amount of bandwidth that the FortiGate can process.

Each NP4 processor connects to the integrated switch fabric through two XAUI links: XAUI0 and XAUI1. All of the odd numbered Ethernet interfaces use XAU0 and all of the even numbered interfaces use XAUI1:

NPU1

XAUI0 = port1,port3,port13, port15, port17

XAUI1 = port2, port4, port14, port16

NPU2

XAUI0 = port5, port7, port18, port20, port22

XAUI1 = port6, port8, port19, port21

NPU3

XAUI0 = port9, port11, port23, port25, port27

XAUI1 = port10, port12, port24, port26, port28

Usually you do not have to be concerned about XAUI link mapping. However, if a FortiGate-3600C NP4 interface is processing a very high amount of traffic you should distribute that traffic among both of the XAUI links connected to it. So if you have a very high volume of traffic flowing between two networks you should connect both networks to the same NP4 processor but to different XAUI links. For example, you could connect one network to Etherent port5 and the other network to Ethernet port6. In this configuration, the second NP4 processor would handle traffic acceleration and both XAUI links would be processing traffic.

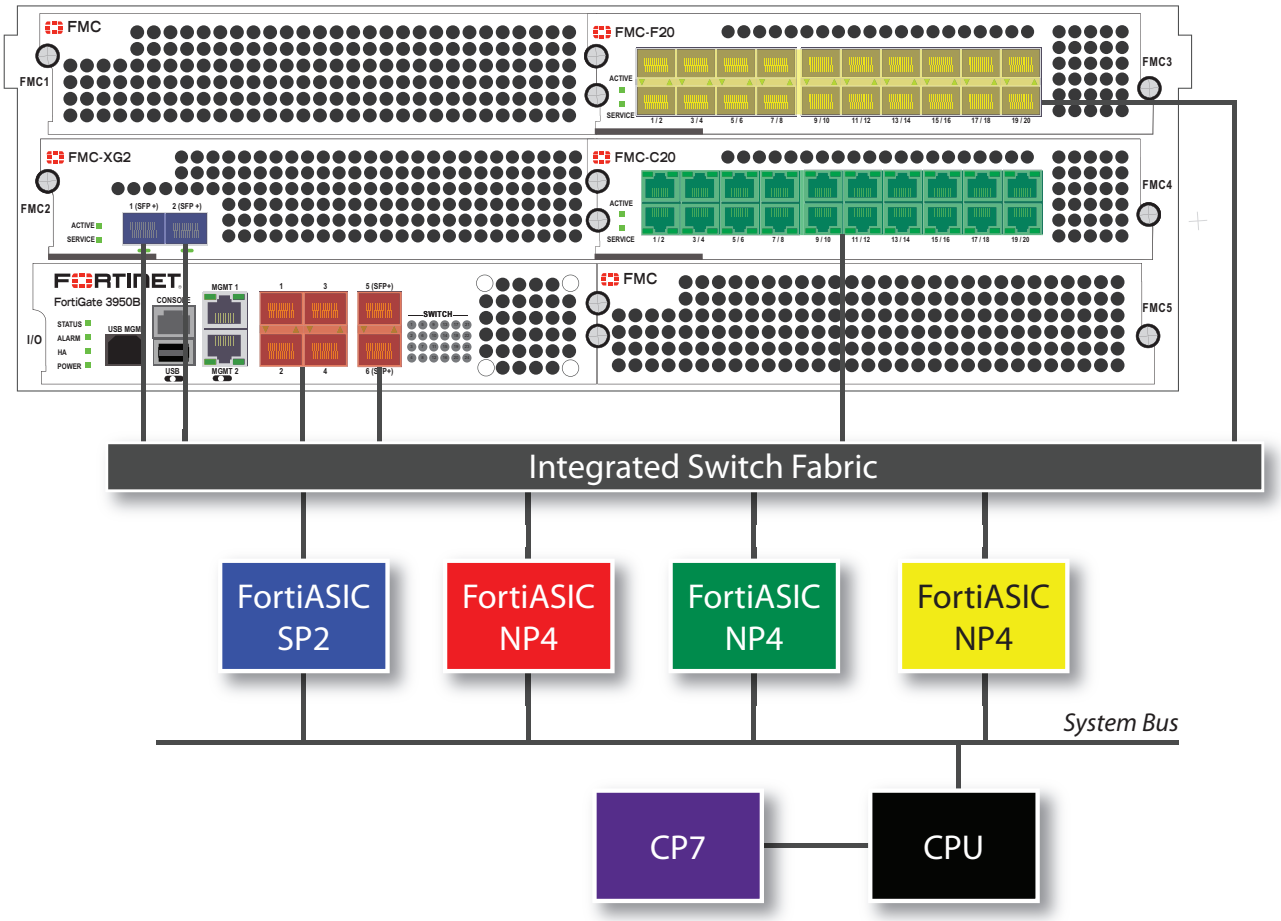
FortiGate-3950B and FortiGate-3951B

The FortiGate-3950B features one NP4 processor. The 1Gb SPF interfaces, port1, port2, port3, port4, and the 10Gb SPF+ interfaces, port5, port6, share connections to one NP4 processor. The FortiGate-3951B is similar to the FortiGate-3950B, except it trades one FMC slot for four FSM slots. The network interfaces available on each model are identical.

You can add additional FMC interface modules. The diagram below shows a FortiGate-3950B with three modules installed: an FMC-XG2, an FMC-F20, and an FMC-C20.

- The FMC-XG2 has one SP2 processor. The 10Gb SPF+ interfaces, port1 and port2, share connections to the processor.
- The FMC-F20 has one NP4 processor and the twenty 1Gb SPF interfaces, port1 through port20, share connections to the NP4 processor.

- The FMC-C20 has one NP4 processor and the twenty 10/100/1000 interfaces, port1 through port20, share connections to the NP4 processor.



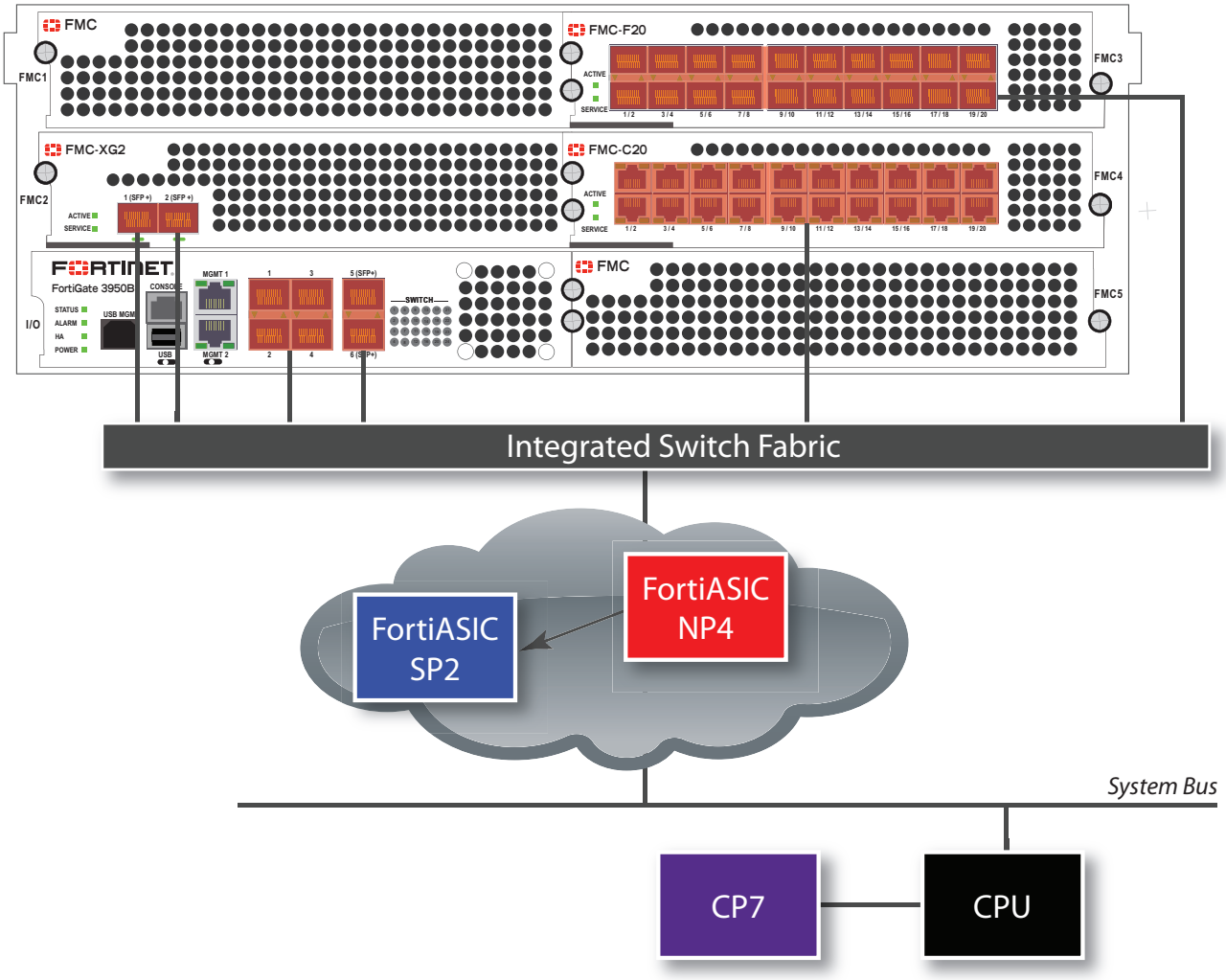
FortiGate-3950B and FortiGate-3951B — load balance mode

Adding one or more FMC-XG2 modules to your FortiGate-3950B allows you to enable load balance mode. This feature allows you increased flexibility in how you use the interfaces on the FortiGate unit. The FortiGate-3951B is similar to the FortiGate-3950B, except it trades one FMC slot for four FSM slots. The network interfaces available on each model are identical.

When enabled, traffic between any two interfaces (excluding management and console) is accelerated whether they are the six interfaces on the FortiGate-3950B itself, or on any installed FMC modules. Traffic is not limited to entering and leaving the FortiGate unit in specific interface groupings to benefit from NP4 and SP2 acceleration. You can use any pair of interfaces.

Security acceleration in this mode is limited, however. Only IPS scanning is accelerated in load balance mode.

The FortiGate-3950B in load balance mode



To enable this feature, issue this CLI command.

```
config system global
```

```
    set sp-load-balance enable
end
```

The FortiGate unit will then restart.

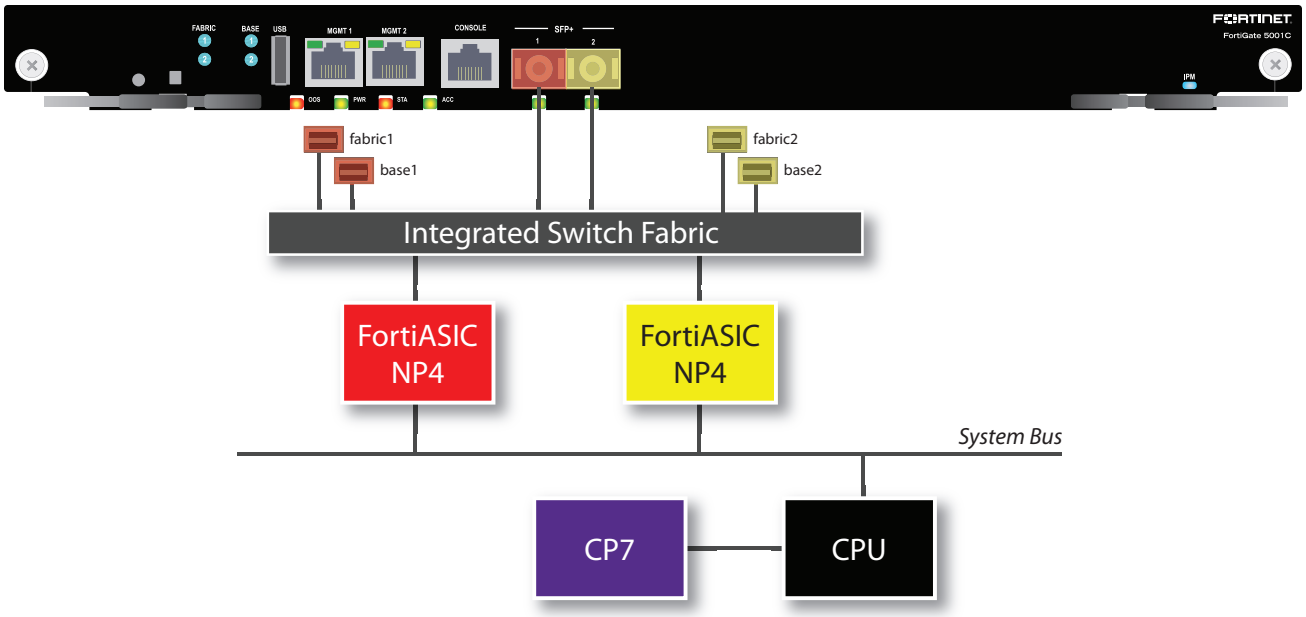
To return to the default mode, issue this CLI command.

```
config system global
    set sp-load-balance disable
end
```

FortiGate-5001C

The FortiGate-5001C board includes two NP4 processors connected to an integrated switch fabric:

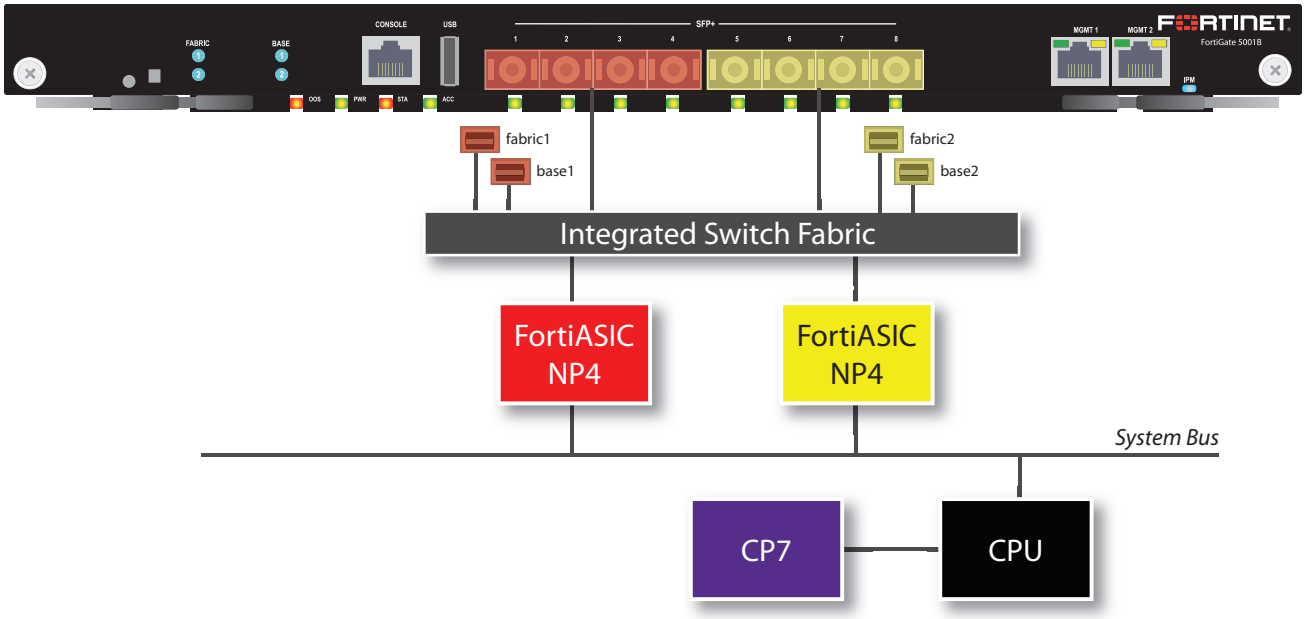
- The port1, fabric1, and base1 interfaces are connected to one NP4 processor.
- The port2, fabric2, and base2 interfaces are connected to the other NP4 processor.



FortiGate-5001B

The FortiGate-5001B board includes two NP4 connected to an integrated switch fabric.

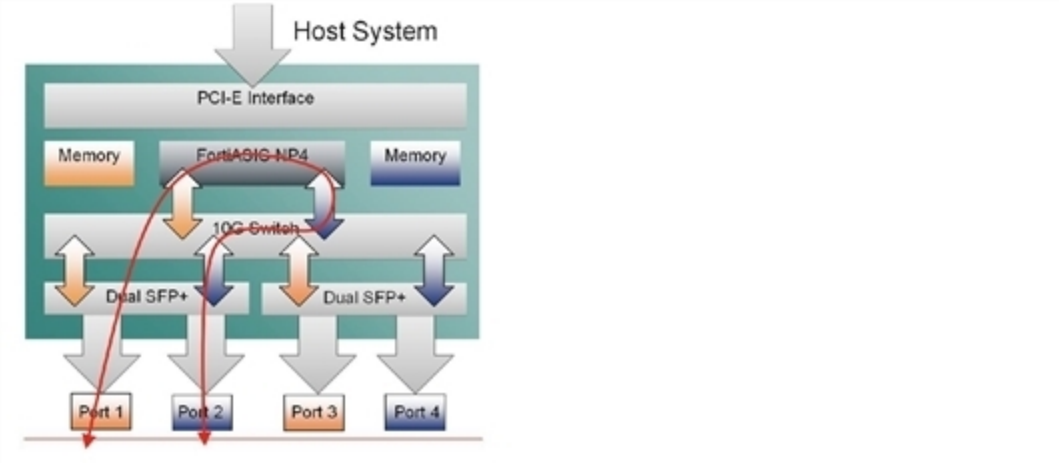
- The port1, port2, port3, port4, fabric1 and base1 interfaces are connected to one NP4 processor.
- The port5, port6, port7, port8, fabric2 and base2 interfaces are connected to the other NP4 processor.



Setting switch-mode mapping on the ADM-XD4

The ADM-XD4 SP has four 10Gb/s ports, but the NP4 processor it contains has only two 10Gb/s ports. The external ports you use are important to optimize the SP for your application.

ADM-XD4 mapping mode



Ports 1 and 3 share one NP4 processor and ports 2 and 4 share the other. Performance ports sharing the same NP4 processor is far better than when forcing network data to move between NP4 processors by using one port from each, for example ports 1 and 2 or ports 3 and 4.

Hardware acceleration diagnose commands

This section describes some diagnose commands you can use to display useful information about sessions processed by NP6 and other NPx processors.

diagnose sys session/session6 list (IPv4, IP6, NAT46, NAT64, and IPsec session information)

Display information about the IPv4, IPv6, NAT46, NAT64 and IPsec sessions being processed by NPx processors. The command output includes the following:

- `offload=1/1` for NP1(FA1) sessions.
- `offload=2/2` for NP1(FA2) sessions.
- `offload=3/3` for NP2 sessions.
- `offload=4/4` for NP4 sessions.
- `offload=5/5` for XLR sessions.
- `offload=6/6` for Nplite/NP4lite sessions.
- `offload=7/7` for XLP sessions.
- `offload=8/8` for NP6 sessions.

- `flag 0x81` means regular traffic.
- `flag 0x82` means IPsec traffic.

Example IPv4 NP6 session

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=2 expire=3597 timeout=3600 flag-
s=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=13->14/14->13 gwy-
y=10.1.100.11/172.16.200.55
hook=pre dir=org act=noop 172.16.200.55:57975->10.1.100.11:80(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.11:80->172.16.200.55:57975(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=04051918 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=137/136, ipid-
d=136/137, vlan=0/0
```

Example IPv4 IPsec NP6 session

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=34 expire=3565 timeout=3600 flag-
s=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/p1-vdom2
state=re may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=57->7/7->57 gwy-
y=10.1.100.11/11.11.11.1
hook=pre dir=org act=noop 172.16.200.55:35254->10.1.100.11:80(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.11:80->172.16.200.55:35254(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=4
serial=00002d29 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=172.16.200.55, bps=260
npu_state=00000000
npu info: flag=0x81/0x82, offload=8/8, ips_offload=0/0, epid=1/3, ipid=3/1, vlan-
n=32779/0
```

Example IPv6 NP6 session

```
diagnose sys session6 list
session6 info: proto=6 proto_state=01 duration=2 expire=3597 timeout=3600 flag-
s=00000000 sockport=0 sockflag=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0
policy_dir=0 tunnel=/
state=may_dirty npu
statistic(bytes/packets/allow_err): org=152/2/0 reply=152/2/0 tuples=2
speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=13->14/14->13
hook=pre dir=org act=noop 2000:172:16:200::55:59145 ->2000:10:1:100::11:80(:::0)
hook=post dir=reply act=noop 2000:10:1:100::11:80 ->2000:172:16:200::55:59145
(:::0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0 serial=0000027a
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=137/136, ipid-
d=136/137, vlan=0/0
```

Example NAT46 NP6 session

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=19 expire=3580 timeout=3600 flag-
s=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=npu nlb
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
speed(Bps/kbps): 0/0
orgin->sink: org nataf->post, reply pre->org dev=52->14/14->52 gwy-
y=0.0.0.0/10.1.100.1
hook=5 dir=org act=noop 10.1.100.1:21937->10.1.100.11:80(0.0.0.0:0)
hook=6 dir=reply act=noop 10.1.100.11:80->10.1.100.1:21937(0.0.0.0:0)
hook=pre dir=org act=noop 2000:172:16:200::55:33945 ->64:ff9b::a01:640b:80(:::0)
hook=post dir=reply act=noop 64:ff9b::a01:640b:80 ->2000:172:16:200::55:33945
(:::0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=04051aae tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x81/0x00, offload=0/8, ips_offload=0/0, epid=0/136, ipid=0/137,
vlan=0/0
```

Example NAT64 NP6 session

```
diagnose sys session6 list
session6 info: proto=6 proto_state=01 duration=36 expire=3563 timeout=3600 flag-
s=00000000 sockport=0 sockflag=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0
policy_dir=0 tunnel=/
state=may_dirty npu nlb
statistic(bytes/packets/allow_err): org=72/1/0 reply=152/2/0 tuples=2
speed(Bps/kbps): 0/0
orgin->sink: org pre->org, reply nataf->post dev=13->14/14->13
hook=pre dir=org act=noop 2000:172:16:200::55:33945 ->64:ff9b::a01:640b:80(:::0)
hook=post dir=reply act=noop 64:ff9b::a01:640b:80 ->2000:172:16:200::55:33945
(:::0)
hook=5 dir=org act=noop 10.1.100.1:21937->10.1.100.11:80(0.0.0.0:0)
hook=6 dir=reply act=noop 10.1.100.11:80->10.1.100.1:21937(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0 serial=0000027b
npu_state=00000000
npu info: flag=0x00/0x81, offload=8/0, ips_offload=0/0, epid=137/0, ipid=136/0,
vlan=0/0
```

diagnose npu np6 session-stats <np6-id> (number of NP6 IPv4 and IPv6 sessions)

You can use the `diagnose npu np6 portlist` command to list the NP6-ids and the interfaces that each NP6 is connected to. The <np6-id> of np6_0 is 0, the <np6-id> of np6_1 is 1 and so on. The `diagnose npu np6 session-stats <np6-id>` command output incudes the following headings:

- `ins44` installed IPv4 sessions
- `ins46` installed NAT46 sessions
- `del4` deleted IPv4 and NAT46 sessions
- `ins64` installed NAT64 sessions
- `ins66` installed IPv6 sessions
- `del6` deleted IPv6 and NAT64 sessions
- `e` is the error counter for each session type

```
diagnose npu np6 session-stats 0
qid    ins44       ins46       del4        ins64       ins66       del6
       ins44_e     ins46_e     del4_e      ins64_e     ins66_e     del6_e
---------------- ---------- ---------- ---------- ---------- ----------
0      94          0           44          0           40          30
       0           0           0           0           0           0
1      84          0           32          0           30          28
       0           0           0           0           0           0
2      90          0           42          0           40          30
       0           0           0           0           0           0
3      86          0           32          0           24          27
       0           0           0           0           0           0
4      72          0           34          0           34          28
       0           0           0           0           0           0
5      86          0           30          0           28          32
       0           0           0           0           0           0
6      82          0           38          0           32          34
       0           0           0           0           0           0
7      86          0           30          0           30          30
       0           0           0           0           0           0
8      78          0           26          0           36          26
       0           0           0           0           0           0
9      86          0           34          0           32          32
       0           0           0           0           0           0
---------------- ---------- ---------- ---------- ---------- ----------
Total  844         0           342         0           326         297
       0           0           0           0           0           0
---------------- ---------- ---------- ---------- ---------- ----------
```

diagnose npu np6 ipsec-stats (NP6 IPsec statistics)

The command output includes IPv4, IPv6, and NAT46 IPsec information:

- spi_ses4 is the IPv4 counter
- spi_ses6 is the IPv6 counter
- 4to6_ses is the NAT46 counter

```
diagnose npu np6 ipsec-stats
vif_start_oid       03ed       vif_end_oid         03fc
IPsec Virtual interface stats:
vif_get             00000000000        vif_get_expired     00000000000
vif_get_fail        00000000000        vif_get_invld       00000000000
vif_set             00000000000        vif_set_fail        00000000000
vif_clear           00000000000        vif_clear_fail      00000000000
np6_0:
sa_install          00000000000        sa_ins_fail         00000000000
sa_remove           00000000000        sa_del_fail         00000000000
4to6_ses_ins        00000000000        4to6_ses_ins_fail   00000000000
4to6_ses_del        00000000000        4to6_ses_del_fail   00000000000
spi_ses6_ins        00000000000        spi_ses6_ins_fail   00000000000
spi_ses6_del        00000000000        spi_ses6_del_fail   00000000000
spi_ses4_ins        00000000000        spi_ses4_ins_fail   00000000000
spi_ses4_del        00000000000        spi_ses4_del_fail   00000000000
sa_map_alloc_fail   00000000000        vif_alloc_fail      00000000000
sa_ins_null_adapter 00000000000        sa_del_null_adapter 00000000000
del_sa_mismatch     00000000000        ib_chk_null_adpt    00000000000
ib_chk_null_sa      00000000000        ob_chk_null_adpt    00000000000
ob_chk_null_sa      00000000000        rx_vif_miss         00000000000
rx_sa_miss          00000000000        rx_mark_miss        00000000000
waiting_ib_sa       00000000000        sa_mismatch         00000000000
msg_miss            00000000000
np6_1:
sa_install          00000000000        sa_ins_fail         00000000000
sa_remove           00000000000        sa_del_fail         00000000000
4to6_ses_ins        00000000000        4to6_ses_ins_fail   00000000000
4to6_ses_del        00000000000        4to6_ses_del_fail   00000000000
spi_ses6_ins        00000000000        spi_ses6_ins_fail   00000000000
spi_ses6_del        00000000000        spi_ses6_del_fail   00000000000
spi_ses4_ins        00000000000        spi_ses4_ins_fail   00000000000
spi_ses4_del        00000000000        spi_ses4_del_fail   00000000000
sa_map_alloc_fail   00000000000        vif_alloc_fail      00000000000
sa_ins_null_adapter 00000000000        sa_del_null_adapter 00000000000
del_sa_mismatch     00000000000        ib_chk_null_adpt    00000000000
ib_chk_null_sa      00000000000        ob_chk_null_adpt    00000000000
ob_chk_null_sa      00000000000        rx_vif_miss         00000000000
rx_sa_miss          00000000000        rx_mark_miss        00000000000
waiting_ib_sa       00000000000        sa_mismatch         00000000000
msg_miss            00000000000
```

diagnose sys mcast-session/session6 list (IPv4 and IPv6 multicast sessions)

This command lists all IPv4 or IPv6 multicast sessions. If a multicast session can be offloaded, the output includes the `offloadable` tag. If the multicast path can be offloaded one of the paths in the command output is tagged as `offloaded`.

The only way to determine the number of offloaded multicast sessions is to use the `diagnose sys mcast-session/session6 list` command and count the number of sessions with the `offload` tag.

```
diagnose sys mcast-session list
session info: id=3 vf=0 proto=17 172.16.200.55.51108->239.1.1.1.7878
used=2 path=11 duration=1 expire=178 indev=6 pkts=2 state:2cpu offloadable
npu-info in-pid=0 vifid=0 in-vtag=0 npuid=0 queue=0 tae=0

path: 2cpu policy=1, outdev=2
        out-vtag=0
path: 2cpu policy=1, outdev=3
        out-vtag=0
path: offloaded policy=1, outdev=7
        out-vtag=0
path: policy=1, outdev=8
        out-vtag=0
path: policy=1, outdev=9
        out-vtag=0
path: policy=1, outdev=10
        out-vtag=0
path: policy=1, outdev=11
        out-vtag=0
path: policy=1, outdev=12
        out-vtag=0
path: policy=1, outdev=13
        out-vtag=0
path: 2cpu policy=1, outdev=64
      out-vtag=0
path: 2cpu policy=1, outdev=68
      out-vtag=0
```

diagnose npu np6 sse-stats <np6-id> (number of NP6 sessions and dropped sessions)

This command displays the total number of inserted, deleted and purged sessions processed by a selected NP6 processor. The number of dropped sessions of each type cam be determined by subtracting the number of successfull sessions from the total number of sessions. For example, the total number of dropped insert sessions is `insert-total - insert-success`.

```
diagnose npu np6 sse-stats 0
Counters         SSE0             SSE1             Total
---------------- ---------------- ---------------- ----------------
active           0                0                0
insert-total     25               0                0
insert-success   25               0                0
delete-total     25               0                0
delete-success   25               0                0
purge-total      0                0                0
purge-success    0                0                0
search-total     40956            38049            79005
search-hit       37714            29867            67581
---------------- ---------------- ---------------- ----------------
pht-size         8421376          8421376
oft-size         8355840          8355840
oftfree          8355839          8355839
PBA              3001
```

diagnose npu np6 dce <np6-id> (number of dropped NP6 packets)

This command displays the number of dropped packets for the selected NP6 processor.

- `IHP1_PKTCHK` number of dropped IP packets
- `IPSEC0_ENGINB0` number of dropped IPSec
- `TPE_SHAPER` number of dropped traffic sharper packets

```
diagnose npu np6 dce 1
IHP1_PKTCHK :0000000000001833 [5b] IPSEC0_ENGINB0 :0000000000000003 [80]
TPE_SHAPER :0000000000000552 [94]
```

diagnose hardware deviceinfo nic <interfac-name> (number of packets dropped by an interface)

This command displays a wide variety of statistics for FortiGate interfaces. The fields `Host Rx dropped` and `Host Tx dropped` display the number of received and trasmitted packets that have been dropped.

```
diagnose hardware deviceinfo nic port2
...
============ Counters ===========
Rx Pkts          :20482043
Rx Bytes         :31047522516
Tx Pkts          :19000495
Tx Bytes         :1393316953
Host Rx Pkts     :27324
Host Rx Bytes    :1602755
Host Rx dropped :0
Host Tx Pkts     :8741
Host Tx Bytes    :5731300
Host Tx dropped :0
sw_rx_pkts       :20482043
sw_rx_bytes      :31047522516
sw_tx_pkts       :19000495
sw_tx_bytes      :1393316953
sw_np_rx_pkts    :19000495
sw_np_rx_bytes   :1469318933
sw_np_tx_pkts    :20482042
sw_np_tx_bytes   :31129450620
```

dianose npu np6 synproxy-stats (NP6 SYN-proxied sessions and unacknowledged SYNs)

This command display information about NP6 syn-proxy sessions including the total number proxied sessions. As well the `Number of attacks, no ACK from client` shows the total number of unacknowledge SYNs.

```
diagnose npu np6 synproxy-stats
DoS SYN-Proxy:
Number of proxied TCP connections : 39277346
Number of working proxied TCP connections : 182860
Number of retired TCP connections : 39094486
Number of attacks, no ACK from client : 208
```

Chapter 13 - High Availability

This FortiOS Handbook chapter contains the following sections:

Solving the High Availability problem describes the high availability problem and introduces the FortiOS solutions described in this document (FGCP, VRRP, and standalone session synchronization).

An introduction to the FGCP introduces the FGCP clustering protocol and many of its features and terminology.

FGCP configuration examples and troubleshooting describes configuring HA clusters and contains HA clustering configuration examples.

Virtual clusters describes configuring HA virtual clusters and contains virtual clustering configuration examples.

Full mesh HA describes configuring FortiGate Full mesh HA and contains a full mesh HA configuration example.

Operating a cluster describes how to operate a cluster and includes detailed information about how various FortiGate systems operate differently in a cluster.

HA and failover protection describes in detail how FortiGate HA device failover, link failover, and session failover work.

HA and load balancing describes how FGCP HA active-active load balancing works and how to configure it.

HA with FortiGate-VM and third-party products describes how FortiGate units interact with third-party products.

VRRPdescribes FortiOS support of the Virtual Router Redundancy Protocol (VRRP) and its use for high availability.

FortiGate Session Life Support Protocol (FGSP) describes how to use the FGSP feature to support using external routers or load balancers to distribute or load balance sessions between two peer FortiGate units.

Configuring FRUP describes how to set up a FortiGate Redundant UTM Protocol (FRUP) cluster consisting of two FortiGate-100D units.

FortiOS 5.2 HA new features

New FortiOS 5.2 HA features are described in the following sections:

- An introduction to the FGCP on page 1270.
- DHCP and PPPoE supported for HA clusters, An introduction to the FGCP on page 1270.
- IPv6 Management Interface Gateway, Configuring the reserved management interface and SNMP remote management of individual cluster units on page 1423.
- IKEv2 Message ID synchronization and failover support, Synchronizing IPsec VPN SAs on page 1484.
- Synchronizing GTP Tunnel sessions and GTP tunnel failover support, FortiOS Carrier GTP session failover on page 1500.
- New VRRP features VRRP on page 1528 and Using a Second Destination IP (VRDST) on page 1531.

Solving the High Availability problem

The basic high availability (HA) problem for TCP/IP networks and security gateways is keeping network traffic flowing. Uninterrupted traffic flow is a critical component for online systems and media because critical business processes quickly come to a halt when the network is down.

The security gateway is a crucial component of most networks since all traffic passes through it. A standalone network security gateway is a single point of failure that is vulnerable to any number of software or hardware problems that could compromise the device and bring all traffic on the network to a halt.

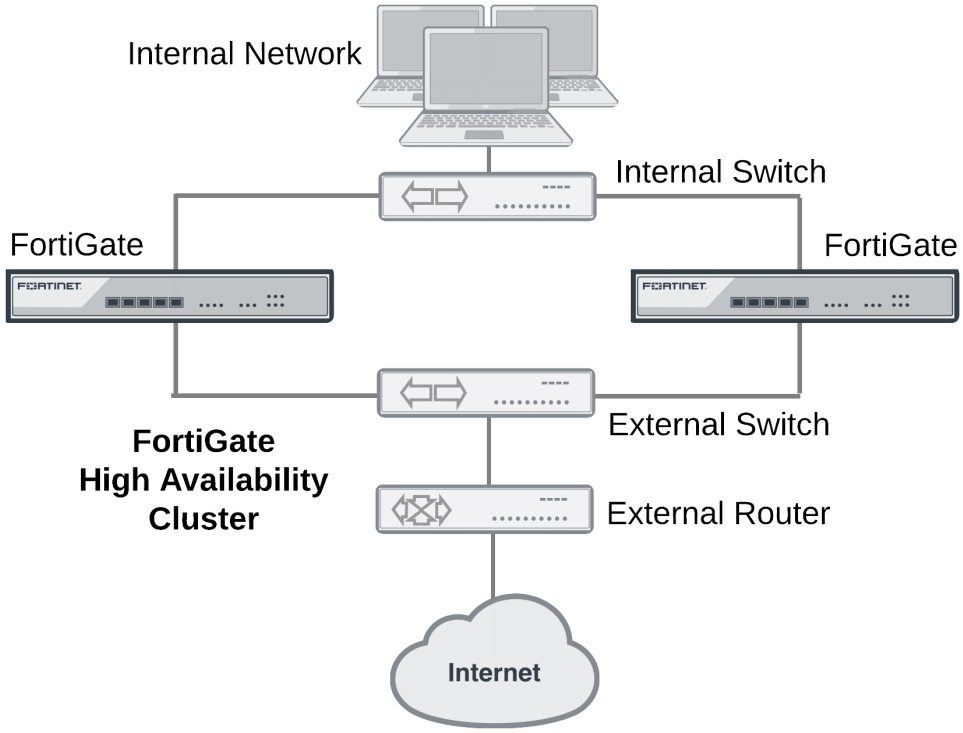
A common solution to the high availability problem is to eliminate the security gateway as single point of failure by introducing redundancy. With two or more redundant security gateways, if one fails, the remaining one or more gateways keep the traffic flowing. FortiOS provides four redundancy solutions: industry standard VRRP as well as three proprietary solutions: FortiGate Cluster Protocol (FGCP) high availability, FortiGate Session Life Support Protocol (FGSP) high availability, and the Fortinet Redundant UTM protocol (FRUP) high availability.

You can combine more than one high availability solution into a single configuration. A common reason for doing this could be to add VRRP to an FGCP or FGSP configuration.

A strong and flexible High availability solution is required for many mission-critical firewall and security profile applications. Each FortiOS high availability solution can be fine tuned to fit into many different network scenarios.

FortiGate Cluster Protocol (FGCP)

FGCP HA provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance. Enhanced reliability is achieved through device failover protection, link failover protection and remote link failover protection. Also contributing to enhanced reliability is session failover protection for most IPv4 and IPv6 sessions including TCP, UDP, ICMP, IPsec VPN, and NAT sessions. Increased performance is achieved though active-active HA load balancing. Extended FGCP features include full mesh HA and virtual clustering. You can also fine tune the performance of the FGCP to change how a cluster forms and shares information among cluster units and how the cluster responds to failures.

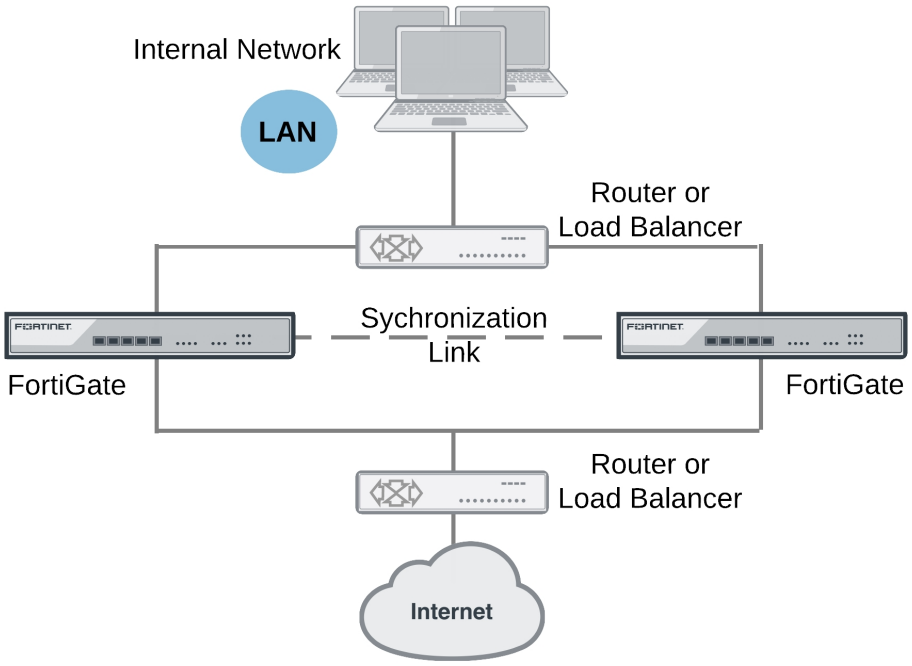


When configured onto your network an FGCP cluster appears to be a single FortiGate unit operating in NAT/Route or Transparent mode and configuration synchronization allows you to configure a cluster in the same way as a standalone FortiGate unit. If a failover occurs, the cluster recovers quickly and automatically and also sends administrator notifications so that the problem that caused the failure can be corrected and any failed equipment restored.

The FGCP is compatible with most network environments and most networking equipment. While initial configuration is relatively quick and easy, a large number of tools and configuration options are available to fine tune the cluster for most situations.

FortiGate Session Life Support Protocol (FGSP)

In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two identical FortiGate units can be integrated into the load balancing configuration using the FortiGate Session Life Support Protocol (FGSP). The external load balancers or routers can distribute sessions among the FortiGate units and the FGSP performs session synchronization of IPv4 and IPv6 TCP, UDP, ICMP, expectation, and NAT sessions to keep the session tables of both FortiGate units synchronized.



If one of the FortiGate units fails, session failover occurs and active sessions fail over to the unit that is still operating. This failover occurs without any loss of data. As well, the external load balancers or routers detect the failover and re-distribute all sessions to the unit that is still operating.

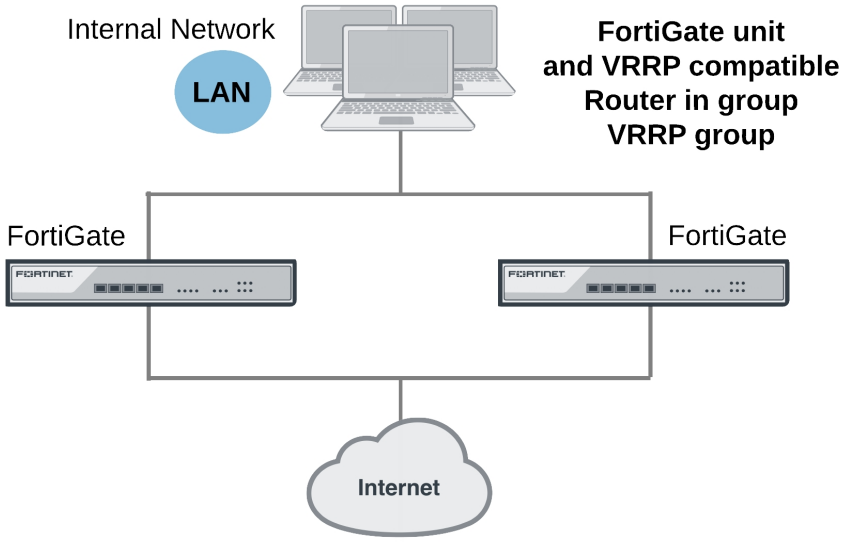
Load balancing and session failover is done by external routers or load balancers and not by the FGSP. The FortiGate units just perform session synchronization which allows session failover to occur without packet loss.

The FGSP also includes configuration synchronization, allowing you to make configuration changes once for both FortiGate units instead of requiring duplicate configuration changes on each unit. Settings that identify the FortiGate unit to the network, for example, interface IP addresses and BGP neighbor settings, are not synchronized so each FortiGate unit maintains its identity on the network. These settings must be configured separately for each FortiGate unit.

In previous versions of FortiOS the FGSP was called TCP session synchronization or standalone session synchronization. However, the FGSP has been expanded to include configuration synchronization and session synchronization of connectionless sessions, expectation sessions, and NAT sessions.

VRRP

FortiGate units can function as master or backup Virtual Router Redundancy Protocol (VRRP) routers and can be quickly and easily integrated into a network that has already deployed VRRP. A FortiGate unit can be integrated into a VRRP group with any third-party VRRP devices and VRRP can provide redundancy between multiple FortiGate units.



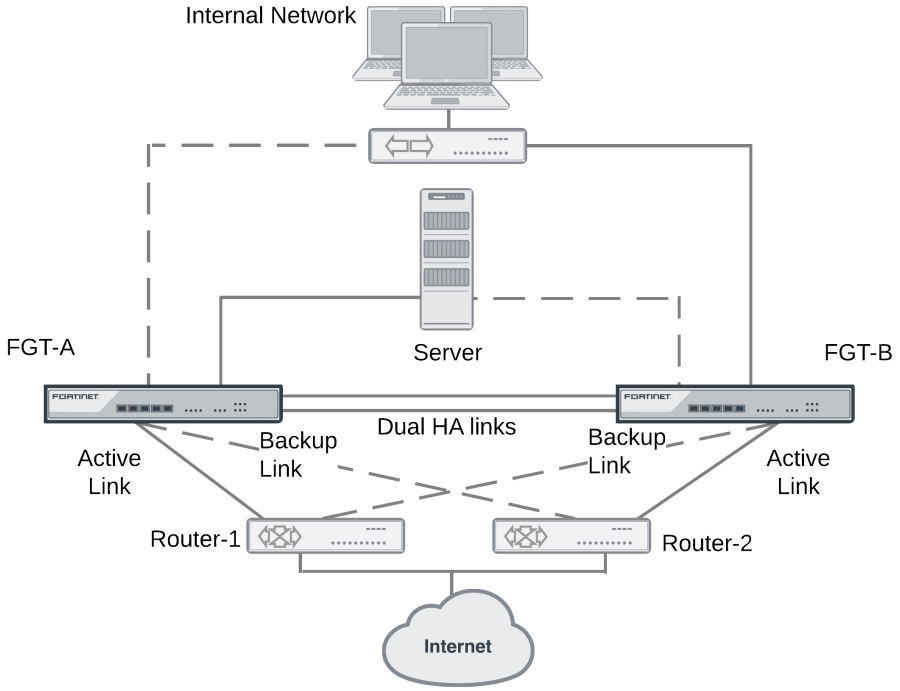
In a VRRP configuration, when a FortiGate unit operating as the master unit fails, a backup unit takes its place and continues processing network traffic. If the backup unit is a FortiGate unit, the network continues to benefit from FortiOS security features. If the backup unit is a router, after a failure traffic will continue to flow, but FortiOS security features will be unavailable until the FortiGate unit is back on line. You can include different FortiGate models in the same VRRP group.

FortiOS supports VRRP between two or more FortiGate units and between FortiGate units and third-party routers that support VRRP. Using VRRP you can assign VRRP routers as master or backup routers. The master router processes traffic and the backup routers monitor the master router and can begin forwarding traffic if the master fails. Similar to the FGCP you can configuration VRRP between multiple FortiGate units to provide redundancy. You can also create a VRRP group with a FortiGate units and any routers that support VRRP.

In a VRRP configuration that consists of one FortiGate unit and one router, normally the FortiGate unit would be the master and all traffic would be processed by the FortiGate unit. If the FortiGate unit fails, all traffic switches to the router. Network connectivity is maintained even though FortiGate security features will be unavailable until the FortiGate unit can is back on line.

Fortinet redundant UTM protocol (FRUP)

An extension to the FGCP combines switching HA and firewall HA into a single unified design. This feature is available on the FortiGate-100D and will be expanded to other models in future releases.



A FRUP setup consists of 2 (and only 2) identical FortiGate-100D units. The setup supports dual redundant HA links between the units for sharing session and configuration data.

FRUP requires redundant external routers where:

- One FortiGate unit has a primary connection to one of the routers and a backup connection to the other.
- The other FortiGate unit has the opposite configuration.

Session-Aware Load Balancing Clustering (SLBC)

Session-Aware Load Balancing Clusters consist of one or more FortiControllers acting as load balancers and FortiGate-5000s and operating as workers all installed in one or two FortiGate-5000 series chassis.

SLBC clusters load balance TCP and UDP sessions. As a session-aware load balancer, the FortiController includes FortiASIC DP processors that maintain state information for all TCP and UDP sessions. The FortiASIC DP processors are capable of directing any TCP or UDP session to any worker installed in the same chassis. This session-awareness means that all TCP and UDP traffic being processed by a specific worker continues to be processed by the same worker. Session-awareness also means that more complex networking features such as network address translation (NAT), fragmented packets, complex UDP protocols, and complex protocols such as SIP that use pinholes, can be load balanced by the cluster.

For more informationa bout SLBC see the *FortiController Session-Aware Load Balancing Guide*.

You cannot mix FGCP and SLBC clusters in the same FortiGate-5000 chassis.

Enhanced Load Balancing Clustering (ELBC)

ELBC uses FortiSwitch-5000 series load balancers to load balance traffic to FortiGate-5000 workers installed in a FortiGate-5000 chassis. ELBC enhances scalability, reliability, and availability of mission critical IP-based services, such as firewall, antivirus, web filtering, IPS, and so on. It also provides high availability by detecting worker failures and automatically redistributing traffic to the workers that are still operating.

ELBC applies a load balancing algorithm against the source and/or destination address of packets to generate a hash key value. Each worker has hash key values assigned to it. If the workers are running, then the traffic is forwarded to the worker assigned to the hash key.The hash key value generated by the algorithm, the hash keys accepted by the worker blades, and the blade the traffic is sent to are automatically calculated by the FortiSwitch.

For more information about ELBC see the *ELBC Configuration Guide*.

You cannot mix FGCP and ELBC clusters in the same FortiGate-5000 chassis.

Content clustering

A content cluster employs FortiSwitch-5203Bs or FortiController-5902Ds to load balance content sessions to FortiGate-5000 workers. FortiSwitch-5203B content clusters consist of one or more FortiSwitch-5203Bs and multiple FortiGate-5001Bs workers. FortiController-5902D content clusters consist of one or more FortiController-5902Ds and multiple FortiGate-5001B workers.

Operating as a FortiGate unit in content cluster mode, a primary FortiSwitch-5203B or FortiController-5902D performs routing, firewalling, stateful inspection, IPsec and SSL VPN encryption/decryption, and other FortiGate functions. The FortiSwitch-5203B includes NP4 processors and the FortiController-5902Ds includes NP6 processors and an integrated switch fabrics that provides fastpath acceleration by offloading communication sessions from the FortiGate CPU.

Using content cluster weighted load balancing, the FortiSwitch-5203Bs or FortiController-5902Ds distribute sessions that require content processing to the workers over the FortiGate-5000 chassis fabric backplane. Content processing sessions include proxy and flow-based security profile functions such as virus scanning, intrusion protection, application control, IPS, web filtering, email filtering, and VoIP. Lload balancing is offloaded to the NP4 or NP6 processors resulting in improved load balancing performance. In some networks, the NP4 or NP6 processors also allow you to configure the efficiently load balance TCP and UDP sessions.

Content cluster mode is similar to active-active HA where the FortiSwitch-5203B or FortiController-5902D operates as the primary unit and load balances security profile sessions to the workers installed in the chassis using weighted load balancing. In this configuration, the HA mode is active-active, the HA load balancing schedule is weight-round-robin and load-balance-all is disabled. You can adjust the HA weighted load balancing weights to change how sessions are load balanced.

You can add a second FortiSwitch-5203B or FortiController-5902D to a content cluster as a backup. The primary FortiSwitch-5203B or FortiController-5902D can load balance sessions to the backup FortiSwitch-5203B or FortiController-5902D as well as the workers. You can control how many sessions are processed by the backup FortiSwitch-5203B or FortiController-5902D by configuring the HA load balancing weights. You can also configure the content cluster to operate the backup FortiSwitch-5203B or FortiController-5902D in standby mode. In this

mode the backup FortiSwitch-5203B or FortiController-5902D does not process any sessions but is just there to take over content clustering if the primary unit fails.

Once the content cluster has been established and all FortiControllers and workers have joined the cluster, you can configure the cluster from the FortiSwitch-5203B or FortiController-5902D GUI or CLI. All configuration changes made to the primary unit are automatically synchronized to all cluster units.

FortiSwitch-5203B or FortiController-5902D firmware upgrades are done from the primaryFortiSwitch-5203B or FortiController-5902D GUI or CLI. Worker firmware upgrades are done from theFortiSwitch-5203B or FortiController-5902D CLI where a single firmware image is uploaded once and synchronized to all of the workers.

An introduction to the FGCP

A FortiGate HA cluster consists of two to four FortiGate units configured for HA operation. Each FortiGate unit in a cluster is called a cluster unit. All cluster units must be the same FortiGate model with the same FortiOS firmware build installed. All cluster units must also have the same hardware configuration (for example, the same AMC modules installed in the same slots, the same number of hard disks and so on) and be running in the same operating mode (NAT/Route mode or Transparent mode).

You can create an FGCP cluster of up to four FortiGate units.

In addition the cluster units must be able to communicate with each other through their heartbeat interfaces. This heartbeat communication is required for the cluster to be created and to continue operating. Without it, the cluster acts like a collection of standalone FortiGate units.

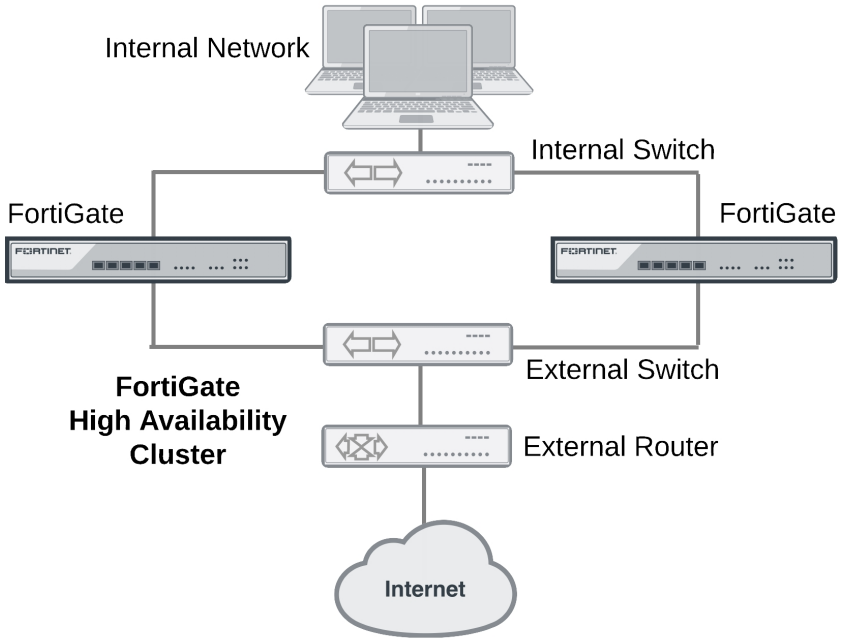
On startup, after configuring the cluster units with the same HA configuration and connecting their heartbeat interfaces, the cluster units use the FortiGate Clustering Protocol (FGCP) to find other FortiGate units configured for HA operation and to negotiate to create a cluster. During cluster operation, the FGCP shares communication and synchronization information among the cluster units over the heartbeat interface link. This communication and synchronization is called the FGCP heartbeat or the HA heartbeat. Often, this is shortened to just heartbeat.

The cluster uses the FGCP to select the primary unit, and to provide device, link and session failover. The FGCP also manages the two HA modes; active-passive (failover HA) and active-active (load balancing HA).

About the FGCP

FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewalling, security profile services, and VPN services.

HA cluster installed between an internal network and the Internet



Inside the cluster the individual FortiGate units are called cluster units. These cluster units share state and configuration information. If one cluster unit fails, the other units in the cluster automatically replace that unit, taking over the work that the failed unit was doing. After the failure, the cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption.

Every FortiGate cluster contains one primary unit (also called the master unit) and one or more subordinate units (also called slave or backup units). The primary unit controls how the cluster operates. The role that the subordinate units play depends on the mode in which the cluster operates: (Active-Passive (AP) or Active-Active (AA).

The ability of an HA cluster to continue providing firewall services after a failure is called failover. FGCP failover means that your network does not have to rely on one FortiGate unit to continue functioning. You can install additional units and form an HA cluster.

A second HA feature, called load balancing, can be used to increase performance. A cluster of FortiGate units can increase overall network performance by sharing the load of processing network traffic and providing security services. The cluster appears to your network to be a single device, adding increased performance without changing your network configuration.

Virtual clustering extends HA features to provide failover protection and load balancing for Virtual Domains (VDOMs). See Virtual clusters on page 1387.

FortiGate models that support redundant interfaces can be configured to support full mesh HA. Full mesh HA is a method of reducing the number of single points of failure on a network that includes an HA cluster. For details about full mesh HA, see Full mesh HA on page 1407.

FGCP failover protection

The FGCP provides IP/MAC takeover for failover protection by assigning virtual MAC addresses to the primary cluster unit and then sending gratuitous ARP packets from the primary unit interfaces to reprogram the network.

Failover times can be less than a second under optimal conditions. You can fine tune failover performance for your network by adjusting cluster status checking timers, routing table update timers, and wait timers.

An HA cluster fails over if the primary unit fails (a device failure) or experiences a link failure. The cluster can detect link failures for connections to the primary unit using port monitoring and for connections between downstream network components using remote IP monitoring. To compensate for a link failover, the cluster maintains active links to keep traffic flowing between high-priority networks. Port and remote IP monitoring can be fine tuned without disrupting cluster operation.

Session Failover

FGCP session failover maintains TCP, SIP and IPsec VPN sessions after a failure. You can also configure session failover to maintain UDP and ICMP sessions. Session failover does not failover multicast, or SSL VPN sessions. Session failover may not be required for all networks because many TCP/IP, UDP, and ICMP protocols can resume sessions on their own. Supporting session failover adds extra overhead to cluster operations and can be disabled to improve cluster performance if it is not required.

Load Balancing

Active-active HA load balances resource-intensive security profile features such as virus scanning, web filtering, intrusion protection, application control, email filtering and data leak prevention operations among all cluster units to provide better performance than a standalone FortiGate unit. If network traffic consists of mainly TCP sessions, the FGCP can also load balance all TCP sessions to improve TCP performance in some network configurations. On some FortiGate models you can also load balance UDP sessions. NP4 and NP6 offloading can accelerate HA load balancing (especially TCP and UDP load balancing). HA load balancing schedules can be adjusted to optimize performance for the traffic mix on your network. Weighted load balancing can be used to control the relative amount of sessions processed by each cluster unit.

Virtual Clustering

Virtual clustering is an extension of the FGCP for a cluster of 2 FortiGate units operating with multiple VDOMS enabled. Not only does virtual clustering provide failover protection for a multiple VDOM configuration, but a virtual cluster can load balance traffic between the cluster units. Load balancing with virtual clustering is quite efficient and load balances all traffic. It is possible to fine tune virtual clustering load balancing in real time to actively optimize load sharing between the cluster units without affecting the smooth operation of the cluster.

Full Mesh HA

High availability improves the reliability of a network by replacing a single point of failure (a single FortiGate unit) with a cluster that can maintain network traffic if one of the cluster units fails. However, in a normal cluster configuration, single points of failure remain. Full mesh HA removes these single points of failure by allowing you to connect redundant switches to each cluster interface. Full mesh HA is achieved by configuring 802.3ad aggregate or redundant interfaces on the FortiGate unit and connecting redundant switches to these interfaces. Configuration is a relatively simple extension of the normal aggregate/redundant interface and HA configurations.

Cluster Management

FortiOS HA provides a wide range of cluster management features:

- Automatic continuous configuration synchronization. You can get a cluster up and running almost as quickly as a standalone FortiGate unit by performing a few basic steps to configure HA settings and minimal network settings on each cluster unit. When the cluster is operating you can configure FortiGate features such as firewalling, content inspection, and VPN in the same way as for a standalone FortiGate unit. All configuration changes (even complex changes such as switching to multiple VDOM mode or from NAT/Route to Transparent mode) are synchronized among all cluster units.
- Firmware upgrades/downgrades. Upgrading or downgrading cluster firmware is similar to upgrading or downgrading standalone FortiGate firmware. The Firmware is uploaded once to the primary unit and the cluster automatically upgrades or downgrades all cluster units in one operation with minimal or no service interruption.
- Individual cluster unit management. In some cases you may want to manage individual cluster units. You can do so from cluster CLI by navigating to each cluster unit. You can also use the reserved management interface feature to give each cluster unit its own IP address and default route. You can use the reserved management interfaces and IP addresses to connect to the GUI and CLI of each cluster unit and configure an SNMP server to poll each cluster unit.
- Removing and adding cluster units. In one simple step any unit (even the primary unit) can be removed from a cluster and given a new IP address. The cluster keeps operating as it was; the transition happening without interrupting cluster operation. A new unit can also be added to an operating cluster without disrupting network traffic. All you have to do is connect the new unit and change its HA configuration to match the cluster's. The cluster automatically finds and adds the unit and synchronizes its configuration with the cluster.
- Debug and diagnose commands. An extensive range of debug and diagnose commands can be used to report on HA operation and find and fix problems.
- Logging and reporting. All cluster units can be configured to record all log messages. These message can be stored on the individual cluster units or sent to a FortiAnalyzer unit. You can view all cluster unit log messages by logging into any cluster unit.
- FortiManager support. FortiManager understands FortiOS HA and automatically recognizes when you add a FortiOS cluster to the FortiManager configuration.

The FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit. This means that in most cases you only have to make a configuration change once to have it synchronized to all cluster units.

Some configuration settings are not synchronized to support some aspects of FortiGate operation. The following settings are not synchronized among cluster units:

- The FortiGate unit host name. Allows you to identify cluster units.
- HA override.
- HA device priority.
- Virtual cluster 1 and Virtual cluster 2 device priorities.
- The HA priority (`ha-priority`) setting for a ping server or dead gateway detection configuration.
- The system interface settings of the FortiGate interface that becomes the HA reserved management interface.
- The default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command.
- The dynamic weighted load balancing thresholds and high and low watermarks.

Synchronizing the configuration (and settings that are not synchronized)

The FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit. This means that in most cases you only have to make a configuration change once to have it synchronized to all cluster units. This includes special configuration settings

that include extra information (for example, 3rd party certificates, replacement message text files and graphics and so on).

Some configuration settings are not synchronized to support some aspects of FortiGate operation. The following settings are not synchronized among cluster units:

- The FortiGate unit host name. Allows you to identify cluster units.
- HA override.
- HA device priority.
- Virtual cluster 1 and Virtual cluster 2 device priorities.
- The HA priority (`ha-priority`) setting for a ping server or dead gateway detection configuration.
- The system interface settings of the FortiGate interface that becomes the HA reserved management interface.
- The default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command.
- The dynamic weighted load balancing thresholds and high and low watermarks.

In addition licenses are not synchronized since FortiGate must be licensed separately. This includes FortiCloud activationand FortiClien licensing, and entering a license key if you purchased more than 10 Virtual Domains (VDOMS). FortiToken licenses can be added at any time because they are synchronized to all cluster members.

Preparing the FortiGates before setting up a FGCP cluster

Before creating an FGCP cluster you should complete the following setup on each FortiGate.

DHCP and PPPoE

Make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.

Firmware version

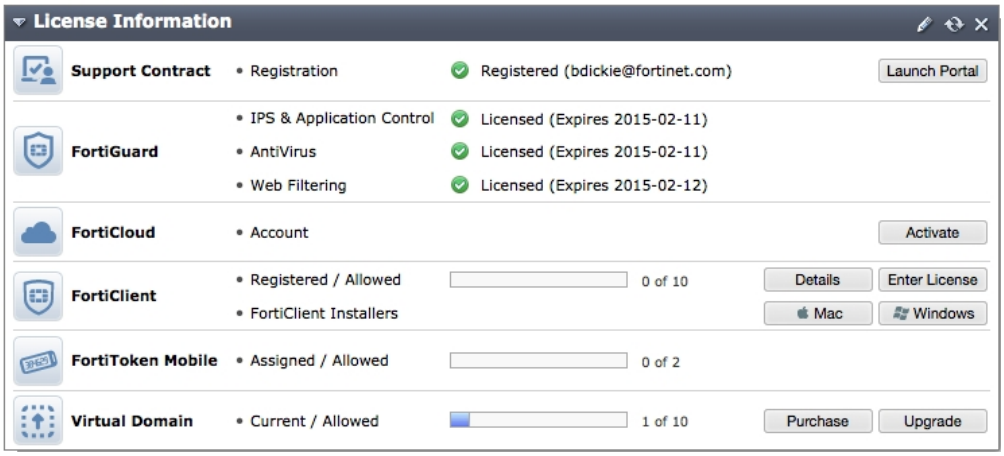
Make sure the FortiGates are running the same FortiOS firmware version.

FortiOS Carrier license

If the FortiGates in the cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Licenses (Support, FortiGuard, FortiCloud, FortiClient, FortiToken Mobile, VDOMs)

Register and apply licenses to each FortiGate. This includes FortiCloud activation and FortiClient licensing, and entering a license key if you purchased more than 10 Virtual Domains (VDOMS). FortiToken licenses can be added at any time because they are synchronized to all cluster members.



Certificates

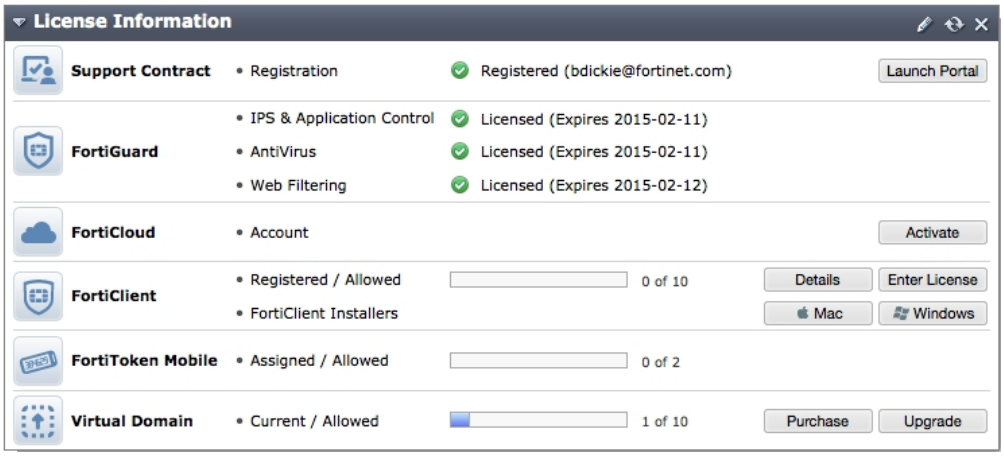
You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.

Configuring FortiGate units for FGCP HA operation

Each FortiGate unit in the cluster must have the same HA configuration. Once the cluster is connected, you can configure it in the same way as you would configure a standalone FortiGate unit. The following example sets the HA mode to active-passive and the HA password to HA_pass.

Make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.

Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to both FortiGates before adding them to the cluster. This includes FortiCloud activation and FortiClient licensing, and entering a license key if you purchased more than 10 Virtual Domains (VDOMS).



You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
FortiToken licenses can be added at any time because they are synchronized to all cluster members.

To configure a FortiGate unit for HA operation - web-based manager

1. Power on the FortiGate unit to be configured.
2. Log into the web-based manager.
3. On the Dashboard **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.
   Changing the host name makes it easier to identify individual cluster units when the cluster is operating.
5. Go to **System > Config > HA** and change the following settings:

Mode	Active-Passive
Group Name	Example_cluster
Password	HA_pass The password must be the same for all FortiGate units in the cluster.

   You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.

6. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select **OK** you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all ARP table entries). You may be able to delete the ARP table of your management PC from a command prompt using a command similar to `arp -d`.
7. Power off the FortiGate unit.
8. Repeat this procedure for all of the FortiGate units in the cluster.
   Once all of the units are configured, continue by connecting the FortiGate HA cluster below.

To configure a FortiGate unit for HA operation - CLI

1. Power on the FortiGate unit to be configured.
2. Log into the CLI.
3. Enter the following command to change the FortiGate unit host name.

```
config system global
   set hostname Example1_host
end
```

   Changing the host name makes it easier to identify individual cluster units when the cluster is operating.

4. Enter the following command to enable HA:

```
config system ha
   set mode active-passive
   set group-name Example_cluster
   set password HA_pass
end
```

   You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.

   The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose connectivity with

the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces. To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

5. Power off the FortiGate unit.
6. Repeat this procedure for all of the FortiGate units in the cluster.
   Once all of the units are configured, continue with connecting the FortiGate HA cluster.

Connecting a FortiGate HA cluster

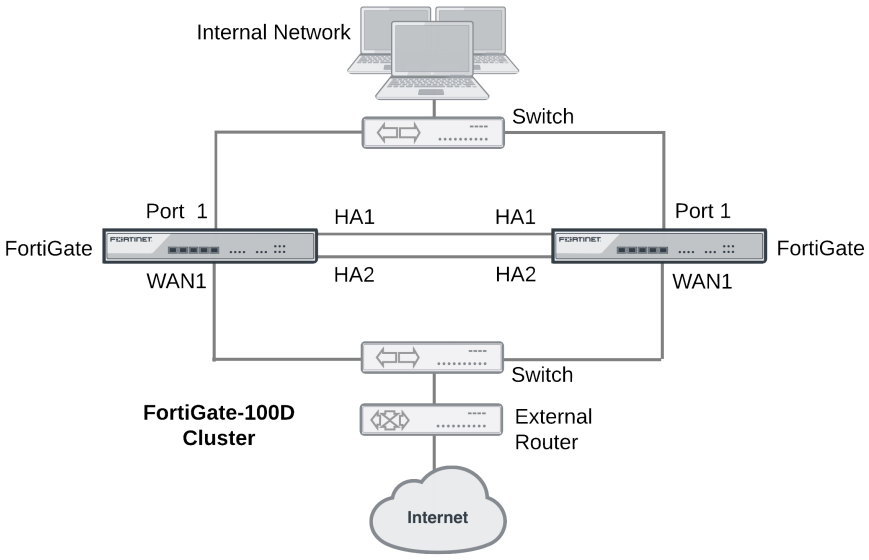
Use the following procedure to connect a cluster. Connect the cluster units to each other and to your network. You must connect all matching interfaces in the cluster to the same switch, then connect these interfaces to their networks using the same switch.

Although you can use hubs, Fortinet recommends using switches for all cluster connections for the best performance.

Connecting an HA cluster to your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual cluster units are functioning and the cluster completes negotiation. Cluster negotiation is automatic and normally takes just a few seconds. During system startup and negotiation all network traffic is dropped.

This section describes how to connect the cluster shownbelow, which consists of two FortiGate-100D units to be connected between the Internet and a head office internal network. The wan1 interfaces of the FortiGate unit connect the cluster to the Internet and the internal interfaces connect the cluster to the internal network. The ha1 and ha2 interfaces are used for redundant HA heartbeat links.

Example cluster connections



To connect a FortiGate HA cluster

1. Connect the WAN1 interfaces of each cluster unit to a switch connected to the Internet.
2. Connect the Port1 interfaces of each cluster unit to a switch connected to the internal network.
3. Connect the HA1 interfaces of the cluster units together. You can use a crossover Ethernet cable or a regular Ethernet cable. (You can also connect the interfaces using Ethernet cables and a switch.)
4. Connect the HA2 interfaces of the cluster units together. You can use a crossover Ethernet cable or a regular Ethernet cable. (You can also connect the interfaces using Ethernet cables and a switch.)
5. Power on both of the FortiGate units.

   As the cluster units start, they negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally just takes a few seconds.

   At least one heartbeat interface should be connected together for the cluster to operate.

   Do not use a switch port for the HA heartbeat traffic. This configuration is not supported.

   You could use one switch to connect all four heartbeat interfaces. However, this is not recommended because if the switch fails both heartbeat interfaces will become disconnected.
6. You can now configure the cluster as if it is a single FortiGate unit.

Active-passive and active-active HA

The first decision to make when configuring FortiGate HA is whether to choose active-passive or active-active HA mode. To configure the HA mode, go to **System > Config > HA** and set Mode to **Active-Passive** or **Active-Active**.

From the CLI enter the following command to set the HA mode to active-passive:

```
config system ha
   set mode a-p
end
```

To form a cluster, all cluster units must be set to the same mode. You can also change the mode after the cluster is up and running. Changing the mode of a functioning cluster causes a slight delay while the cluster renegotiates to operate in the new mode and possibly select a new primary unit.

Active-passive HA (failover protection)

An active-passive (A-P) HA cluster provides hot standby failover protection. An active-passive cluster consists of a primary unit that processes communication sessions, and one or more subordinate units. The subordinate units are connected to the network and to the primary unit but do not process communication sessions. Instead, the subordinate units run in a standby state. In this standby state, the configuration of the subordinate units is synchronized with the configuration of the primary unit and the subordinate units monitor the status of the primary unit.

Active-passive HA provides transparent device failover among cluster units. If a cluster unit fails, another immediately take its place.

Active-passive HA also provides transparent link failover among cluster units. If a cluster unit interface fails or is disconnected, this cluster unit updates the link state database and the cluster negotiates and may select a new primary unit.

If session failover (also called session pickup) is enabled, active-passive HA provides session failover for some communication sessions.

The following example shows how to configure a FortiGate unit for active-passive HA operation. You would enter the exact same commands on every FortiGate unit in the cluster.

```
config system ha
   set mode a-p
   set group-name myname
   set password HApass
end
```

Active-active HA (load balancing and failover protection)

By default, active-active HA load balancing distributes proxy-based security profile processing to all cluster units. Proxy-based security profile processing is CPU and memory-intensive, so FGCP load balancing may result in higher throughput because resource-intensive processing is distributed among all cluster units.

Normally, sessions accepted by policies that don't include security proflies are not load balanced and are processed by the primary unit. You can configure active-active HA to load balance additional sessions.

An active-active HA cluster consists of a primary unit that receives all communication sessions and load balances them among the primary unit and all of the subordinate units. In an active-active cluster the subordinate units are also considered active since they also process content processing sessions. In all other ways active-active HA operates the same as active-passive HA.

The following example shows how to configure a FortiGate unit for active-active HA operation. You would enter the exact same commands on every FortiGate unit in the cluster.

```
config system ha
   set mode a-a
   set group-name myname
   set password HApass
end
```

Identifying the cluster and cluster units

You can use the cluster group name, group id, and password to identify a cluster and distinguish one cluster from another. If you have more than one cluster on the same network, each cluster must have a different group name, group id, and password.

Group name

Use the group name to identify the cluster. The maximum length of the group name is 32 characters. The group name must be the same for all cluster units before the cluster units can form a cluster. After a cluster is operating, you can change the group name. The group name change is synchronized to all cluster units. The group name appears on the FortiGate dashboard of a functioning cluster as the **Cluster Name**.

To add or change the group name from the web-based manager go to **Config > System > HA** and change the **Group Name**.

Enter the following CLI command to change the group name to Cluster_name:

```
config system ha
   set group-name Cluster_name
end
```

Password

Use the password to identify the cluster. You should always change the password when configuring a cluster. The password must be the same for all FortiGate units before they can form a cluster. When the cluster is operating you can change the password, if required. Two clusters on the same network cannot have the same password.

To change the password from the web-based manager go to **Config > System > HA** and change the **Password**.

Enter the following CLI command to change the password to ha_pwd:

```
config system ha
   set password ha_pwd
end
```

Group ID

Similar to the group name, the group ID is also identifies the cluster. In most cases you do not have to change the group ID. However, you should change the group ID if you have more than one cluster on the same network. All members of the HA cluster must have the same group ID. The group ID is a number from 0 to 255.

Changing the group ID changes the cluster virtual MAC address. If two clusters on the same network have the same group ID you may encounter MAC address conflicts.

Enter the following CLI command to change the group ID to 10:

```
config system ha
   set group-id 10
end
```

Device failover, link failover, and session failover

The FGCP provides transparent device and link failover. You can also enable session pickup to provide session failover. A failover can be caused by a hardware failure, a software failure, or something as simple as a network cable being disconnected causing a link failover. When a failover occurs, the cluster detects and recognizes the failure and takes steps to respond so that the network can continue to operate without interruption. The internal operation of the cluster changes, but network components outside of the cluster notice little or no change.

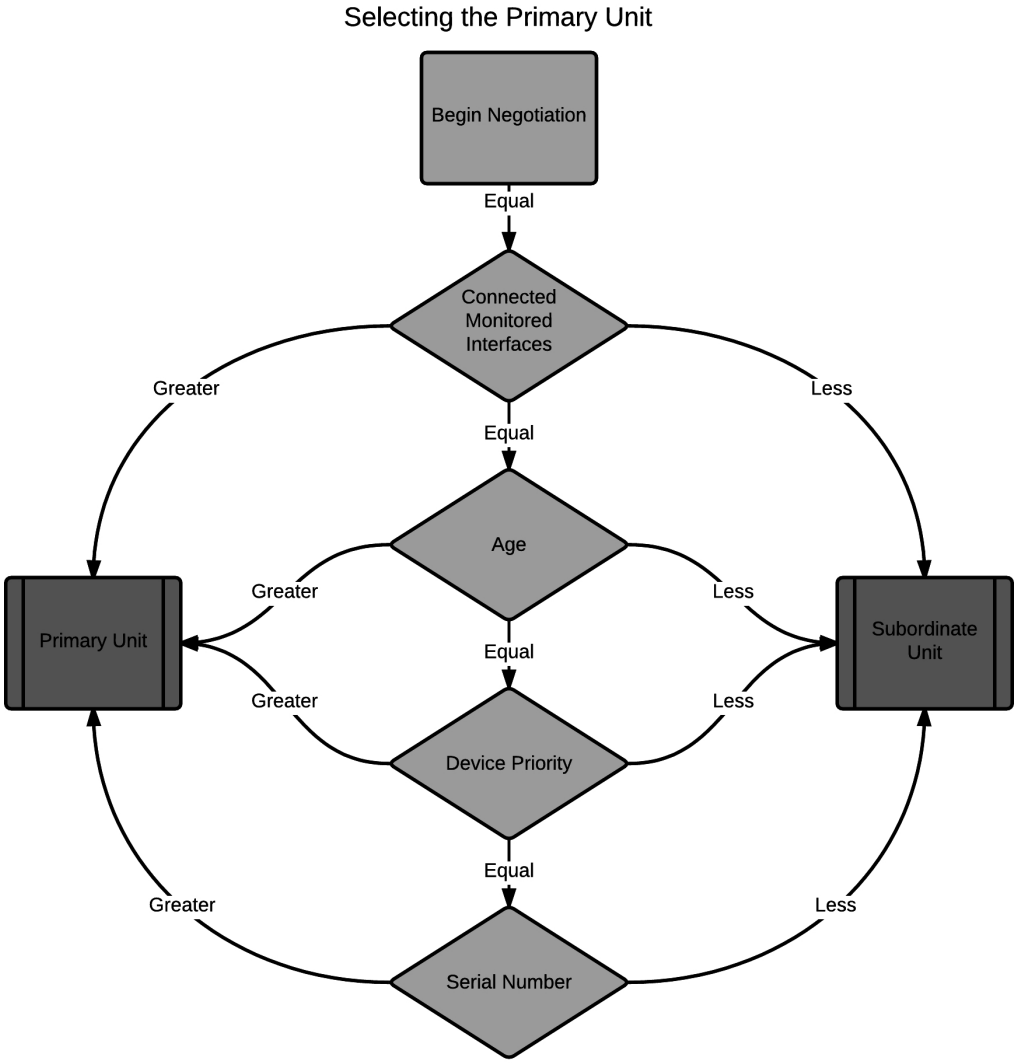
If a failover occurs, the cluster also records log messages about the event and can be configured to send log messages to a syslog server and to a FortiAnalyzer unit. The cluster can also send SNMP traps and alert email messages. These alerts can notify network administrators of the failover and may contain information that the network administrators can use to find and fix the problem that caused the failure.

For a complete description of device failover, link failover, and session failover, how clusters support these types of failover, and how FortiGate HA clusters compensate for a failure to maintain network traffic flow see HA and failover protection on page 1455.

Primary unit selection

Once FortiGate units recognize that they can form a cluster, the cluster units negotiate to select a primary unit. Primary unit selection occurs automatically based on the criteria shown below. After the cluster selects the primary unit, all of the remaining cluster units become subordinate units.

Negotiation and primary unit selection also takes place if a primary unit fails (device failover) or if a monitored interface fails or is disconnected (link failover). During a device or link failover, the cluster renegotiates to select a new primary unit also using the criteria shown below.



For many basic HA configurations primary unit selection simply selects the cluster unit with the highest serial number to become the primary unit. A basic HA configuration involves setting the HA mode to active-passive or active-active and configuring the cluster group name and password. Using this configuration, the cluster unit with the highest serial number becomes the primary unit because primary unit selection disregards connected monitored interfaces (because interface monitoring is not configured), the age of the cluster units would usually always be the same, and all units would have the same device priority.

Using the serial number is a convenient way to differentiate cluster units; so basing primary unit selection on the serial number is predictable and easy to understand and interpret. Also the cluster unit with the highest serial number would usually be the newest FortiGate unit with the most recent hardware version. In many cases you may not need active control over primary unit selection, so basic primary unit selection based on serial number is sufficient.

In some situations you may want have control over which cluster unit becomes the primary unit. You can control primary unit selection by setting the device priority of one cluster unit to be higher than the device priority of all other cluster units. If you change one or more device priorities, during negotiation, the cluster unit with the highest device priority becomes the primary unit. As shown above, the FGCP selects the primary unit based on device priority before serial number. For more information about how to use device priorities, see Primary unit selection and device priority on page 1285.

The only other way that you can influence primary unit selection is by configuring interface monitoring (also called port monitoring). Using interface monitoring you can make sure that cluster units with failed or disconnected monitored interfaces cannot become the primary unit. See Primary unit selection and monitored interfaces on page 1282.

Finally, the age of a cluster unit is determined by a number of operating factors. Normally the age of all cluster units is the same so normally age has no effect on primary unit selection. Age does affect primary unit selection after a monitored interface failure. For more information about age, see Primary unit selection and age on page 1282.

Primary unit selection and monitored interfaces

If you have configured interface monitoring the cluster unit with the highest number of monitored interfaces that are connected to networks becomes the primary unit. Put another way, the cluster unit with the highest number of failed or disconnected monitored interfaces cannot become the primary unit.

Normally, when a cluster starts up, all monitored interfaces of all cluster units are connected and functioning normally. So monitored interfaces do not usually affect primary unit selection when the cluster first starts.

A cluster always renegotiates when a monitored interface fails or is disconnected (called link failover). A cluster also always renegotiates when a failed or disconnected monitored interface is restored.

If a primary unit monitored interface fails or is disconnected, the cluster renegotiates and if this is the only failed or disconnected monitored interface the cluster selects a new primary unit.

If a subordinate unit monitored interface fails or is disconnected, the cluster also renegotiates but will not necessarily select a new primary unit. However, the subordinate unit with the failed or disconnected monitored interface cannot become the primary unit.

Multiple monitored interfaces can fail or become disconnected on more than one cluster unit. Each time a monitored interface is disconnected or fails, the cluster negotiates to select the cluster unit with the most connected and operating monitored interfaces to become the primary unit. In fact, the intent of the link failover feature is just this, to make sure that the primary unit is always the cluster unit with the most connected and operating monitored interfaces.

Primary unit selection and age

The cluster unit with the highest age value becomes the primary unit. The age of a cluster unit is the amount of time since a monitored interface failed or is disconnected. Age is also reset when a cluster unit starts (boots up). So, when all cluster units start up at about the same time, they all have the same age. Age does not affect primary unit selection when all cluster units start up at the same time. Age also takes precedence over priority for primary unit selection.

If a link failure of a monitored interface occurs, the age value for the cluster unit that experiences the link failure is reset. So, the cluster unit that experienced the link failure also has a lower age value than the other cluster units. This reduced age does not effect primary unit selection because the number of link failures takes precedence over the age.

If the failed monitored interface is restored the cluster unit that had the failed monitored interface cannot become the primary unit because its age is still lower than the age of the other cluster units.

In most cases, the way that age is handled by the cluster reduces the number of times the cluster selects a new primary unit, which results in a more stable cluster since selecting a new primary unit has the potential to disrupt traffic.

Cluster age difference margin (grace period)

In any cluster, some of the cluster units may take longer to start up than others. This startup time difference can happen as a result of a number of issues and does not affect the normal operation of the cluster. To make sure that cluster units that start slower can still become primary units, by default the FGCP ignores age differences of up to 5 minutes (300 seconds).

In most cases, during normal operation this age difference margin or grace period helps clusters function as expected. However, the age difference margin can result in some unexpected behavior in some cases:

- During a cluster firmware upgrade with `uninterruptible-upgrade` enabled (the default configuration) the cluster should not select a new primary unit after the firmware of all cluster units has been updated. But since the age difference of the cluster units is most likely less than 300 seconds, age is not used to affect primary unit selection and the cluster may select a new primary unit.
- During failover testing where cluster units are failed over repeatedly the age difference between the cluster units will most likely be less than 5 minutes. During normal operation, if a failover occurs, when the failed unit rejoins the cluster its age will be very different from the age of the still operating cluster units so the cluster will not select a new primary unit. However, if a unit fails and is restored in a very short time the age difference may be less than 5 minutes. As a result the cluster may select a new primary unit during some failover testing scenarios.

Changing the cluster age difference margin

You can change the cluster age difference margin using the following command:

```
config system ha
   set ha-uptime-diff-margin 60
end
```

This command sets the cluster age difference margin to 60 seconds (1 minute). The age difference margin range 1 to 65535 seconds. The default is 300 seconds.

You may want to reduce the margin if during failover testing you don't want to wait the default age difference margin of 5 minutes. You may also want to reduce the margin to allow uninterruptible upgrades to work. See Upgrading cluster firmware on page 1439.

You may want to increase the age margin if cluster unit startup time differences are larger than 5 minutes.

Displaying cluster unit age differences

You can use the CLI command `diagnose sys ha dump-by all-vcluster` to display the age difference of the units in a cluster. This command also displays information about a number of HA-related parameters for each cluster unit. You can enter the command from the primary unit CLI or you can enter the command from a subordinate unit after using `execute ha manage` to log into a subordinate unit CLI. The information displayed by the command is relative to the unit that you enter the command from.

For example, a cluster of two FortiGate-5001C units with no changes to the default HA configuration except to enable port monitoring for port1. Entering the `diagnose sys ha dump-by all-vcluster` command from the primary unit CLI displays information similar to the following:

```
diagnose sys ha dump-by all-vcluster
      HA information.
vcluster id=1, nventry=2, state=work, digest=4.e8.62.17.7b.1d...
ventry idx=0,id=1,FG-5KC3E13800084,prio=128,0,claimed=0,override=0,
   flag=0x01,time=0,mon=0
   mondev=port1,50
ventry idx=1,id=1,FG-5KC3E13800051,prio=128,0,claimed=0,override=0,
   flag=0x00,time=189,mon=0
```

The command displays one `ventry` line for each cluster unit. The first `ventry` in the example contains information for the cluster unit that you are logged into (usually the primary unit). The other `ventry` lines contain information for the other units in the cluster (in the example there is only one other cluster unit). The command also includes a `mondev` entry that displays the interface monitoring configuration.

The `time` field is always `0` for the unit that you are logged into. The `time` field for the other cluster unit is the age difference between the unit that you are logged into and the other cluster unit. The age difference is in the form seconds/10.

In the example, the age of the subordinate unit is 18.9 seconds more than the age of the primary unit. The age difference is less than 5 minutes (less than 300 seconds) so age has no affect on primary unit selection. The cluster selected the unit with the highest serial number to be the primary unit.

If you use `execute ha manage 1` to log into the subordinate unit CLI and enter `diagnose sys ha dump 1` you get results similar to the following:

```
diagnose sys ha dump-by all-vcluster
      HA information.
vcluster id=1, nventry=2, state=standby, digest=4.e8.62.17.7b.1d...
ventry idx=1,id=1,FG-5KC3E13800051,prio=128,0,claimed=0,override=0,
   flag=0x01,time=0,mon=0
   mondev=port1,50
ventry idx=0,id=1,FG-5KC3E13800084,prio=128,0,claimed=1,override=0,
   flag=0x00,time=-189,mon=0
```

The `time` for the primary unit is `-189`, indicating that age of the subordinate unit age is 18.9 seconds higher than the primary unit age.

If port1 (the monitored interface) of the primary unit is disconnected, the cluster renegotiates and the former subordinate unit becomes the primary unit. When you log into the new primary unit CLI and enter `diagnose sys ha dump-by all-vcluster` you could get results similar to the following:

```
diagnose sys ha dump-by all-vcluster
      HA information.
vcluster id=1, nventry=2, state=work, digest=3.f8.d1.63.4d.d2...
ventry idx=0,id=1,FG-5KC3E13800046,prio=128,0,claimed=0,
   override=0,flag=1,time=0,mon=0
   mondev=port1,50
ventry idx=1,id=1,FG-5KC3E13800084,prio=128,-50,claimed=0,
   override=0,flag=0,time=1362,mon=0
```

The command results show that the age of the new primary unit is 136.2 seconds higher than the age of the new subordinate unit.

If port1 of the former primary unit is reconnected the cluster will once again make this the primary unit because the age difference will still be less than 300 seconds. When you log into the primary unit CLI and enter `diagnose sys ha dump-by all-vcluster` you get results similar to the following:

```
diagnose sys ha dump-by all-vcluster
      HA information.
vcluster id=1, nventry=2, state=work, digest=4.a5.60.11.cf.d4...
ventry idx=0,id=1,FG-5KC3E13800084,prio=128,0,claimed=0,
   override=0,flag=1,time=0,mon=0
   mondev=port1,50
ventry idx=1,id=1,FG-5KC3E13800046,prio=128,0,claimed=0,
   override=0,flag=0,time=-1362,mon=0
```

Resetting the age of all cluster units

In some cases, age differences among cluster units can result in the wrong cluster unit or the wrong virtual cluster becoming the primary unit. For example, if a cluster unit set to a high priority reboots, that unit will have a lower age than other cluster units when it rejoins the cluster. Since age takes precedence over priority, the priority of this cluster unit will not be a factor in primary unit selection.

This problem also affects virtual cluster VDOM partitioning in a similar way. After a reboot of one of the units in a virtual cluster configuration, traffic for all VDOMs could continue to be processed by the cluster unit that did not reboot. This can happen because the age of both virtual clusters on the unit that did not reboot is greater that the age of both virtual clusters on the unit that rebooted.

One way to resolve this issue is to reboot all of the cluster units at the same time so that the age of all of the cluster units is reset. However, rebooting cluster units may interrupt or at least slow down traffic. If you would rather not reboot all of the cluster units you can instead use the following command to reset the age of individual cluster units.

```
diagnose sys ha reset-uptime
```

This command resets the age of a unit back to zero so that if no other unit in the cluster was reset at the same time, it will now have the lowest age. You would use this command to reset the age of the cluster unit that is currently the primary unit. Since it will have the lowest age, the other unit in the cluster will have the highest age and can then become the primary unit.

The `diagnose sys ha reset-uptime` command should only be used as a temporary solution. The command resets the HA age internally and does not affect the up time displayed for cluster units using the `diagnose sys ha dump-by all-vcluster` command or the up time displayed on the Dashboard or cluster members list. To make sure the actual up time for cluster units is the same as the HA age you should reboot the cluster units during a maintenance window.

Primary unit selection and device priority

A cluster unit with the highest device priority becomes the primary unit when the cluster starts up or renegotiates. By default, the device priority for all cluster units is 128. You can change the device priority to control which FortiGate unit becomes the primary unit during cluster negotiation. All other factors that influence primary unit selection either cannot be configured (age and serial number) or are synchronized among all cluster units (interface monitoring). You can set a different device priority for each cluster unit. During negotiation, if all monitored interfaces are connected, and all cluster units enter the cluster at the same time (or have the same age), the cluster with the highest device priority becomes the primary unit.

A higher device priority does not affect primary unit selection for a cluster unit with the most failed monitored interfaces or with an age that is higher than all other cluster units because failed monitored interfaces and age are used to select a primary unit before device priority.

Increasing the device priority of a cluster unit does not always guarantee that this cluster unit will become the primary unit. During cluster operation, an event that may affect primary unit selection may not always result in the cluster renegotiating. For example, when a unit joins a functioning cluster, the cluster will not renegotiate. So if a unit with a higher device priority joins a cluster the new unit becomes a subordinate unit until the cluster renegotiates.

Enabling the `override` HA CLI keyword makes changes in device priority more effective by causing the cluster to negotiate more often to make sure that the primary unit is always the unit with the highest device priority. For more information about `override`, see Primary unit selection on page 1280.

Controlling primary unit selection by changing the device priority

You set a different device priority for each cluster unit to control the order in which cluster units become the primary unit when the primary unit fails.

To change the device priority from the web-based manager go to **Config > System > HA** and change the **Device Priority**.

Enter the following CLI command to change the device priority to 200:

```
config system ha
   set priority 200
end
```

The device priority is not synchronized among cluster units. In a functioning cluster you can change the device priority of any unit in the cluster. Whenever you change the device priority of a cluster unit, when the cluster negotiates, the unit with the highest device priority becomes the primary unit.

The following example shows how to change the device priority of a subordinate unit to 255 so that this subordinate unit becomes the primary unit. You can change the device priority of a subordinate unit by going to **Config > System > HA** and selecting the Edit icon for the subordinate unit. Or from the CLI you can use the `execute ha manage 0` command to connect to the highest priority subordinate unit. After you enter the following commands the cluster renegotiates and selects a new primary unit.

```
execute ha manage 1
   config system ha
      set priority 255
   end
```

If you have three units in a cluster you can set the device priorities as shown below. When the cluster starts up, cluster unit A becomes the primary unit because it has the highest device priority. If unit A fails, unit B becomes the primary unit because unit B has a higher device priority than unit C.

Example device priorities for a cluster of three FortiGate units

Cluster unit	Device priority
A	200
B	100
C	50

When configuring HA you do not have to change the device priority of any of the cluster units. If all cluster units have the same device priority, when the cluster first starts up the FGCP negotiates to select the cluster unit with the highest serial number to be the primary unit. Clusters also function normally if all units have the same device priority.

You can change the device priority if you want to control the roles that individual units play in the cluster. For example, if you want the same unit to always become the primary unit, set this unit device priority higher than the device priority of other cluster units. Also, if you want a cluster unit to always become a subordinate unit, set this cluster unit device priority lower than the device priority of other cluster units.

If you have a cluster of three units you can set a different priority for each unit to control which unit becomes the primary unit when all three cluster units and functioning and which will be the primary unit when two cluster units are functioning.

The device priority range is 0 to 255. The default device priority is 128.

If you are configuring a virtual cluster, if you have added virtual domains to both virtual clusters, you can set the device priority that the cluster unit has in virtual cluster 1 and virtual cluster 2. If a FortiGate unit has different device priorities in virtual cluster 1 and virtual cluster 2, the FortiGate unit may be the primary unit in one virtual cluster and the subordinate unit in the other.

Primary unit selection and the FortiGate unit serial number

The cluster unit with the highest serial number is more likely to become the primary unit. When first configuring FortiGate units to be added to a cluster, if you do not change the device priority of any cluster unit, then the cluster unit with the highest serial number always becomes the primary unit.

Age does take precedence over serial number, so if a cluster unit takes longer to join a cluster for some reason (for example if one cluster unit is powered on after the others), that cluster unit will not become the primary unit because the other units have been in the cluster longer.

Device priority and failed monitored interfaces also take precedence over serial number. A higher device priority means a higher priority. So if you set the device priority of one unit higher or if a monitored interface fails, the cluster will not use the FortiGate serial number to select the primary unit.

Points to remember about primary unit selection

Some points to remember about primary unit selection:

- The FGCP compares primary unit selection criteria in the following order: Failed Monitored interfaces > Age > Device Priority > Serial number. The selection process stops at the first criteria that selects one cluster unit.
- Negotiation and primary unit selection is triggered if a cluster unit fails or if a monitored interface fails.

- If the HA age difference is more than 5 minutes (300 seconds), the cluster unit that is operating longer becomes the primary unit.
- If HA age difference is less than 5 minutes (300 seconds), the device priority and FortiGate serial number selects the cluster unit to become the primary unit.
- Every time a monitored interface fails the HA age of the cluster unit is reset to 0.
- Every time a cluster unit restarts the HA age of the cluster unit is reset to 0.

Temporarily setting a cluster unit to be the primary unit

You can use the following diagnose command to set a cluster unit to be the primary unit.

```
diagnose sys ha set-as-master enable
```

This command is intended for demonstration purposes and not for production use. This command may not be visible for all FortiOS versions.

When you enter this command, the cluster immediately re-negotiates and the cluster unit on which you entered this command becomes the primary unit. This change is temporary and will be reverted if the cluster unit restarts.

You can also use the following command from the same cluster unit to turn this option off, causing the cluster to renegotiate and select a new primary unit.

```
diagnose sys ha set-as-master disable
```

You can also configure when to disabling the set-as-master setting. For example, to disable the set as master setting on January 25, 2015 you can enter a date after the disable keyword:

```
diagnose sys ha set-as-master disable 2015 01 25
```

HA override

The HA `override` CLI keyword is disabled by default. When `override` is disabled a cluster may not always renegotiate when an event occurs that affects primary unit selection. For example, when `override` is disabled a cluster will not renegotiate when you change a cluster unit device priority or when you add a new cluster unit to a cluster. This is true even if the unit added to the cluster has a higher device priority than any other unit in the cluster. Also, when `override` is disabled a cluster does not negotiate if the new unit added to the cluster has a failed or disconnected monitored interface.

For a virtual cluster configuration, `override` is enabled by default for both virtual clusters when you enable virtual cluster 2. For more information, see Virtual clustering and HA override on page 1388.

In most cases you should keep `override` disabled to reduce how often the cluster negotiates. Frequent negotiations may cause frequent traffic interruptions.

However, if you want to make sure that the same cluster unit always operates as the primary unit and if you are less concerned about frequent cluster negotiation you can set its device priority higher than other cluster units and enable `override`.

To enable `override`, connect to each cluster unit CLI (using the `execute ha manage` command) and use the `config system ha` CLI command to enable `override`.

For `override` to be effective, you must also set the device priority highest on the cluster unit that you want to always be the primary unit. To increase the device priority, from the CLI use the `config system ha` command and increase the value of the `priority` keyword to a number higher than the default priority of 128.

You can also increase the device priority from the web-based manager by going to **System > Config > HA**. To increase the device priority of the primary unit select edit for the primary or subordinate unit and set the **Device Priority** to a number higher than 128.

The `override` setting and device priority value are not synchronized to all cluster units. You must enable override and adjust device priority manually and separately for each cluster unit.

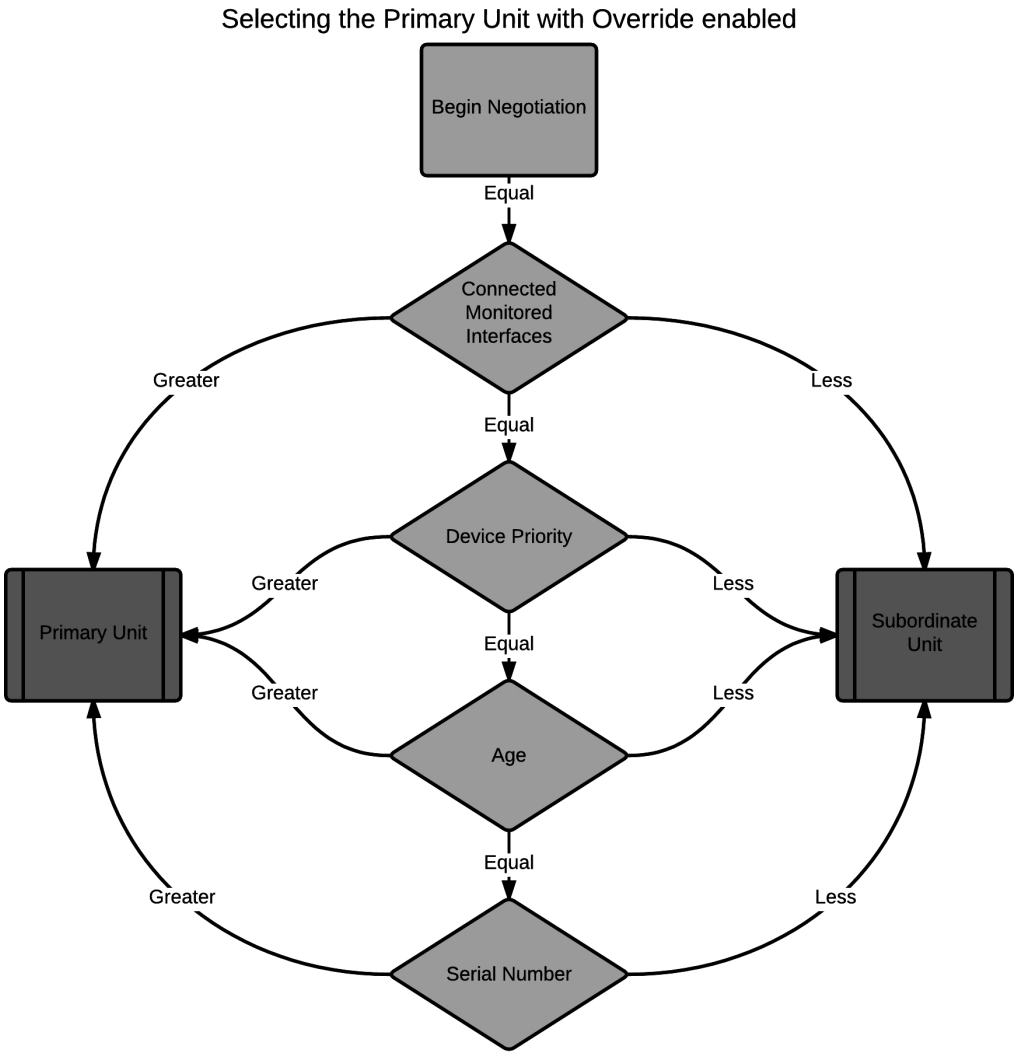
With `override` enabled, the primary unit with the highest device priority will always become the primary unit. Whenever an event occurs that may affect primary unit selection, the cluster negotiates. For example, when `override` is enabled a cluster renegotiates when you change the device priority of any cluster unit or when you add a new unit to a cluster.

Override and primary unit selection

Enabling `override` changes the order of primary unit selection. As shown below, if `override` is enabled, primary unit selection considers device priority before age and serial number. This means that if you set the device priority higher on one cluster unit, with `override` enabled this cluster unit becomes the primary unit even if its age and serial number are lower than other cluster units.

Similar to when `override` is disabled, when `override` is enabled primary unit selection checks for connected monitored interfaces first. So if interface monitoring is enabled, the cluster unit with the most disconnected monitored interfaces cannot become the primary unit, even of the unit has the highest device priority.

If all monitored interfaces are connected (or interface monitoring is not enabled) and the device priority of all cluster units is the same then age and serial number affect primary unit selection.



Controlling primary unit selection using device priority and override

To configure one cluster unit to always become the primary unit you should set its device priority to be higher than the device priorities of the other cluster units and you should enable `override` on all cluster units.

Using this configuration, when the cluster is operating normally the primary unit is always the unit with the highest device priority. If the primary unit fails the cluster renegotiates to select another cluster unit to be the primary unit. If the failed primary unit recovers, starts up again and rejoins the cluster, because `override` is enabled, the cluster renegotiates. Because the restarted primary unit has the highest device priority it once again becomes the primary unit.

In the same situation with `override` disabled, because the age of the failed primary unit is lower than the age of the other cluster units, when the failed primary unit rejoins the cluster it does not become the primary unit. Instead, even though the failed primary unit may have the highest device priority it becomes a subordinate unit because its age is lower than the age of all the other cluster units.

Points to remember about primary unit selection when override is enabled

Some points to remember about primary unit selection when `override` is enabled:

- The FGCP compares primary unit selection criteria in the following order: Failed Monitored Interfaces > Device Priority > Age > Serial number. The selection process stops at the first criteria that selects one cluster unit.
- Negotiation and primary unit selection is triggered whenever an event occurs which may affect primary unit selection. For example negotiation occurs, when you change the device priority, when you add a new unit to a cluster, if a cluster unit fails, or if a monitored interface fails.
- Device priority is considered before age. Otherwise age is handled the same when `override` is enabled.

Configuration changes can be lost if override is enabled

In some cases, when override is enabled and you make configuration changes to an HA cluster these changes can be lost. For example, consider the following sequence:

1. A cluster of two FortiGate units is operating with `override` enabled.
   - FGT-A: Primary unit with device priority 200 and with `override` enabled
   - FGT-B: Subordinate unit with device priority 100 and with `override` disabled
   - If both units are operating, FGT-A always becomes the primary unit because FGT-A has the highest device priority.
2. FGT-A fails and FGT-B becomes the new primary unit.
3. The administrator makes configuration changes to the cluster.
   The configuration changes are made to FGT-B because FGT-B is operating as the primary unit. These configuration changes are not synchronized to FGT-A because FGT-A is not operating.
4. FGT-A is restored and starts up again.
5. The cluster renegotiates and FGT-A becomes the new primary unit.
6. The cluster recognizes that the configurations of FGT-A and FGT-B are not the same.
7. The configuration of FGT-A is synchronized to FGT-B.
   The configuration is always synchronized from the primary unit to the subordinate units.
8. The cluster is now operating with the same configuration as FGT-A. The configuration changes made to FGT-B have been lost.

The solution

When `override` is enabled, you can prevent configuration changes from being lost by doing the following:

- Verify that all cluster units are operating before making configuration changes (from the web-based manager go to **System > Config > HA** to view the cluster members list or from the FortiOS CLI enter `get system ha status`).
- Make sure the device priority of the primary unit is set higher than the device priorities of all other cluster units before making configuration changes.
- Disable `override` either permanently or until all configuration changes have been made and synchronized to all cluster units.

Override and disconnecting a unit from a cluster

A similar scenario to that described above may occur when `override` is enabled and you use the Disconnect from Cluster option from the web-based manager or the `execute ha disconnect` command from the CLI to disconnect a cluster unit from a cluster.

Configuration changes made to the cluster can be lost when you reconnect the disconnected unit to the cluster. You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit. Otherwise, when the disconnected unit joins the cluster, if `override` is enabled, the cluster renegotiates and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units and any configuration changes made between when the unit was disconnected and reconnected are lost.

Delaying how quickly the primary unit rejoins the cluster when override is enabled

In some cases when override is enabled and the unit designated to be the primary unit rejoins the cluster it will become the primary unit too soon and cause traffic disruption. This can happen, for example, if one of the FortiGate interfaces gets its address using PPPoE. If the backup unit is operating as the primary unit and processing traffic, when the primary unit comes up it may need a short time to get a new IP address from the PPPoE server. If the primary unit takes over the cluster before it has an IP address, traffic will be distrupted until the prinary unit gets its address.

You can resolve this problem by using the following command to add a wait time. In this example the wait time is 10 seconds. The wait time range is 0 to 3600 seconds and the default wait time is 0 seconds.

```
config system ha
   set override-wait-time 10
end
```

With this wait time configured, after the primary unit is up and running it has 10 seconds to synchronize sessions, get IP address(es) from PPPoE and DHCP servers and so on. After 10 seconds the primary unit sends gratiutious arp packets and all traffic to the cluster is sent to the new primary unit. You can adjust the wait time according to the conditions on your network.

FortiGate HA compatibility with DHCP and PPPoE

FortiGate HA is compatible with DHCP and PPPoE but care should be taken when configuring a cluster that includes a FortiGate interface configured to get its IP address with DHCP or PPPoE. Fortinet recommends that you turn on DHCP or PPPoE addressing for an interface after the cluster has been configured. If an interface is configured for DHCP or PPPoE, turning on high availability may result in the interface receiving and incorrect address or not being able to connect to the DHCP or PPPoE server correctly.

You cannot switch to operate in HA mode if one or more FortiGate unit interfaces is configured as a PPTP or L2TP client.

You can configure a cluster to act as a DHCP server or a DHCP relay agent. In both active-passive and active-active clusters DHCP relay sessions are always handled by the primary unit. It is possible that a DHCP relay session could be interrupted by a failover. If this occurs the DHCP relay session is not resumed after the failover and the DHCP client may have to repeat the DHCP request.

When a cluster is operating as a DHCP server the primary unit responds to all DHCP requests and maintains the DHCP server address lease database. The cluster also dynamically synchronizes the DHCP server address lease database to the subordinate units. If a failover occurs, the new primary unit will have an up-to-date DHCP server address lease database. Synchronizing the DHCP address lease database prevents the new primary unit from responding incorrectly to new DHCP requests after a failover.

Also, it is possible that when FortiGate units first negotiate to form a cluster that a unit that ends up as a subordinate unit in the cluster will have information in its DHCP address lease database that the cluster unit

operating as the primary unit does note have. This can happen if a FortiGate unit responds to DHCP requests while operating as a standalone unit and then when the cluster is formed this unit becomes a subordinate unit. Because of this possibility, after a cluster is formed the DHCP address lease databases of all of the cluster units are merged into one database which is then synchronized to all cluster units.

HA and distributed clustering

The FGCP supports widely separated cluster units installed in different physical locations. Distributed clusters can have cluster units in different rooms in the same building, different buildings in the same location, or even different geographical sites such as different cities, countries or continents.

Just like any cluster, distributed clusters require heartbeat communication between cluster units. In a distributed cluster this heartbeat communication can take place over the Internet or over other transmission methods including satellite linkups.

Because of the possible distance it may take a relatively long time for heartbeat packets to be transmitted between cluster units. To support a distributed cluster you may need to increase the heartbeat interval so that the cluster expects extra time between heartbeat packets. For information about changing the heartbeat interval and other heartbeat related settings, see Modifying heartbeat timing on page 1462.

Clusters of three or four FortiGate units

The FGCP supports a cluster of two, three, or four FortiGate units. You can add more than two units to a cluster to improve reliability: if two cluster units fail the third will continue to operate and so on. A cluster of three or four units in active-active mode may improve performance since another cluster unit is available for security profile processing. However, active-active FGCP HA results in diminishing performance returns as you add units to the cluster, so the additional performance achieved by adding the third cluster unit may not be worth the cost.

There are no special requirements for clusters of more than two units. Here are a few recommendations though:

- The matching heartbeat interfaces of all of the cluster units must be able to communicate with each other. So each unit's matching heartbeat interface should be connected to the same switch. If the ha1 interface is used for heartbeat communication, then the ha1 interfaces of all of the units in the cluster must be connected together so communication can happen between all of the cluster units over the ha1 interface.
- Redundant heartbeat interfaces are recommended. You can reduce the number of points of failure by connecting each matching set of heartbeat interfaces to a different switch. This is not a requirement; however, and you can connect both heartbeat interfaces of all cluster units to the same switch. However, if that switch fails the cluster will stop forwarding traffic.
- For any cluster, a dedicated switch for each heartbeat interface is recommended because of the large volume of heartbeat traffic and to keep heartbeat traffic off of other networks, but it is not required.
- Full mesh HA can scale to three or four FortiGate units. Full mesh HA is not required if you have more than 2 units in a cluster.
- Virtual clustering can only be done with two FortiGates.

Connecting a cluster of three FortiGate units

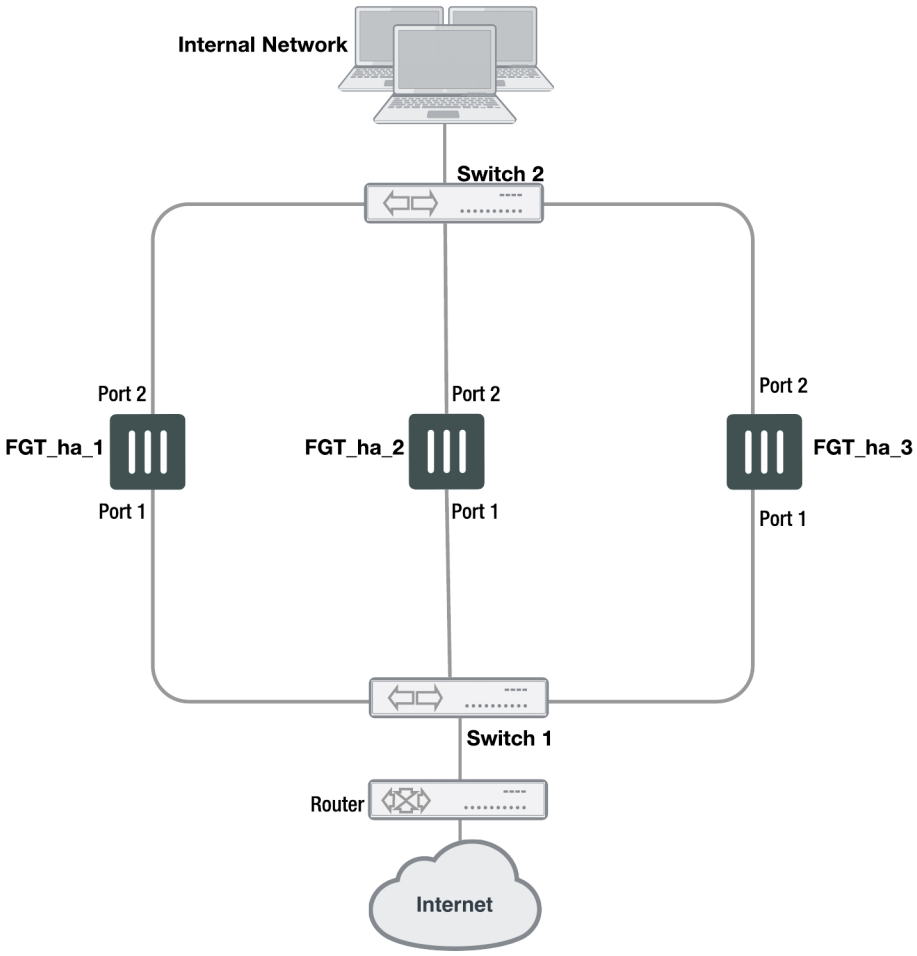
This example shows how to connect a cluster of three FortiGate units where:

- Port1 connects the cluster to the Internet
- Port2 connects the cluster to the internal network
- Port3 and Port4 are the heartbeat interfaces

Use the following steps to connect the cluster units to each other and to their networks:

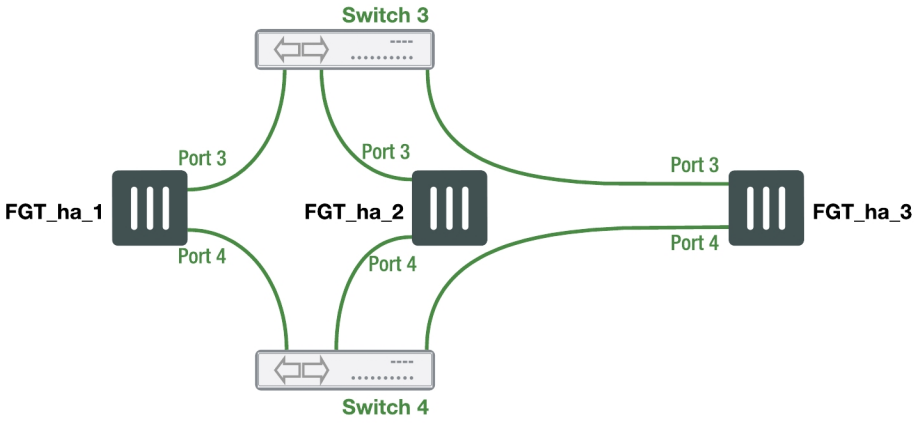
1. Connect the network interfaces:
   - Connect the port1 interface of each FortiGate unit to the same switch (Switch 1) and connect this switch to the Internet.
   - Connect the port2 interface of each FortiGate unit to the same switch (Switch 2) and connect this switch to the internal Network.

Connecting the network interfaces (cluster of three FortiGate units)



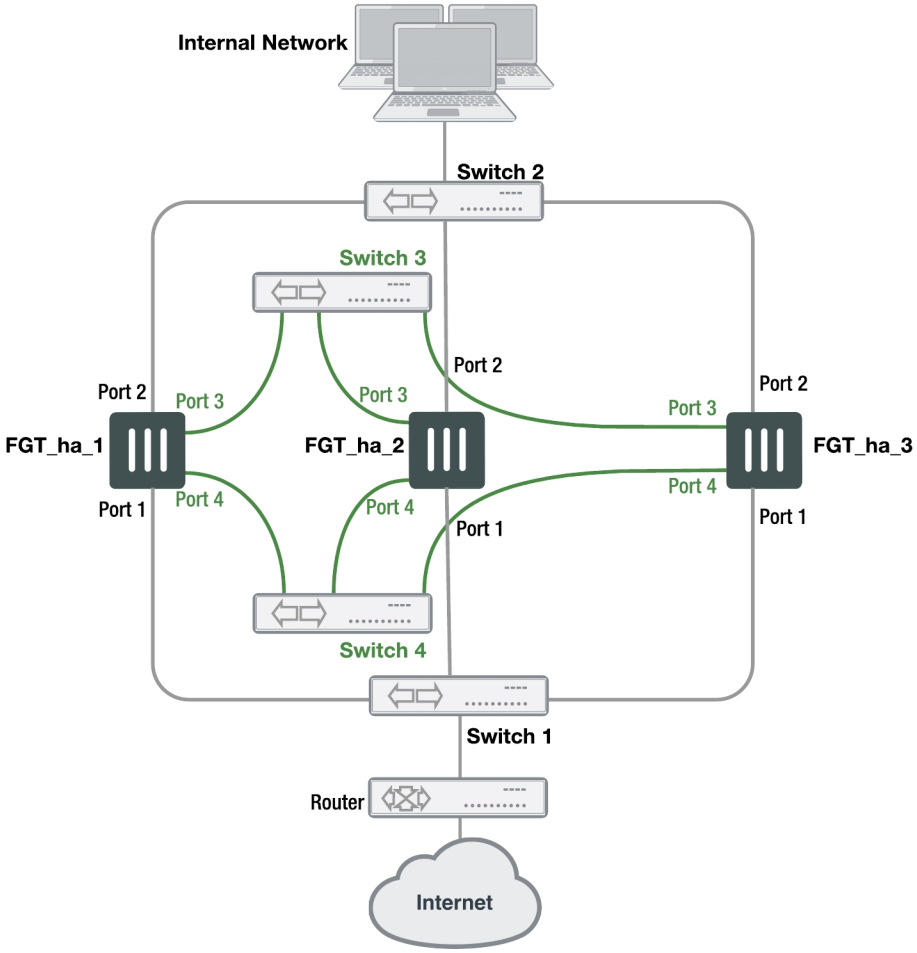
2. Connect the heartbeat interfaces:
   - Connect the port3 interface of each FortiGate unit to the same switch (Switch 3)
   - Connect the port4 interface of each FortiGate unit to the same switch (Switch 4)

Connecting the heartbeat interfaces (cluster of three FortiGate units)



The network and heartbeat connections when combined into one diagram appear like the following:

Network and heartbeat interface connections (cluster of three FortiGate units)



Disk storage configuration and HA

If your cluster units include storage disks (for example for storing log messages, WAN optimization data and web caching) all cluster units must have identical storage disk configurations. This means each cluster unit must have same number of disks (including AMC and FortiGate Storage Module (FSM) hard disks) and also means that matching disks in each cluster unit must be the same size, have the same format, and have the same number of partitions.

In most cases the default hard disk configuration of the cluster units will be compatible. However, a hard disk formatted by an older FortiGate firmware version may not be compatible with a hard disk formatted by a more recent firmware version. Problems may also arise if you have used the `execute scsi-dev` command to add or change hard disk protections.

If a cluster unit CLI displays hard disk compatibility messages, you may need to use the `execute scsi-dev delete` command to delete partitions. You can also use the `execute formatlogdisk` command to

reformat disks. In some cases after deleting all partitions and reformatting the disks, you may still see disk incompatibility messages. If this happens, contact Fortinet Customer Support for assistance.

Heartbeat interfaces

Fortinet suggests the following practices related to heartbeat interfaces:

Do not use a FortiGate switch port for the HA heartbeat traffic. This configuration is not supported.

- For clusters of two FortiGate units, as much as possible, heartbeat interfaces should be directly connected using patch cables (without involving other network equipment such as switches). If switches have to be used they should not be used for other network traffic that could flood the switches and cause heartbeat delays.
  - If you cannot use a dedicated switch, the use of a dedicated VLAN can help limit the broadcast domain to protect the heartbeat traffic and the bandwidth it creates.
- For clusters of three or four FortiGate units, use switches to connect heartbeat interfaces. The corresponding heartbeat interface of each FortiGate unit in the cluster must be connected to the same switch. For improved redundancy use a different switch for each heartbeat interface. In that way if the switch connecting one of the heartbeat interfaces fails or is unplugged, heartbeat traffic can continue on the other heartbeat interfaces and switch.
- Isolate heartbeat interfaces from user networks. Heartbeat packets contain sensitive cluster configuration information and can consume a considerable amount of network bandwidth. If the cluster consists of two FortiGate units, connect the heartbeat interfaces directly using a crossover cable or a regular Ethernet cable. For clusters with more than two units, connect heartbeat interfaces to a separate switch that is not connected to any network.
- If heartbeat traffic cannot be isolated from user networks, enable heartbeat message encryption and authentication to protect cluster information. See Enabling or disabling HA heartbeat encryption and authentication.
- Configure and connect redundant heartbeat interfaces so that if one heartbeat interface fails or becomes disconnected, HA heartbeat traffic can continue to be transmitted using the backup heartbeat interface. If heartbeat communication fails, all cluster members will think they are the primary unit resulting in multiple devices on the network with the same IP addresses and MAC addresses (condition referred to as *Split Brain*) and communication will be disrupted until heartbeat communication can be reestablished.
- Do not monitor dedicated heartbeat interfaces; monitor those interfaces whose failure should trigger a device failover.
- Where possible at least one heartbeat interface should not be connected to an NPx processor to avoid NPx-related problems from affecting heartbeat traffic.

Interface monitoring (port monitoring)

Fortinet suggests the following practices related to interface monitoring (also called port monitoring):

- Wait until a cluster is up and running and all interfaces are connected before enabling interface monitoring. A monitored interface can easily become disconnected during initial setup and cause failovers to occur before the cluster is fully configured and tested.
- Monitor interfaces connected to networks that process high priority traffic so that the cluster maintains connections to these networks if a failure occurs.
- Avoid configuring interface monitoring for all interfaces.

- Supplement interface monitoring with remote link failover. Configure remote link failover to maintain packet flow if a link not directly connected to a cluster unit (for example, between a switch connected to a cluster interface and the network) fails. See Remote link failover.

Troubleshooting

The following sections in this document contain troubleshooting information:

- FGCP configuration examples and troubleshooting on page 1313
- Troubleshooting virtual clustering on page 1406
- Troubleshooting full mesh HA on page 1419
- FortiGate VM for Hyper-V HA configuration on page 1524

FGCP HA terminology

The following HA-specific terms are used in this document.

Cluster

A group of FortiGate units that act as a single virtual FortiGate unit to maintain connectivity even if one of the FortiGate units in the cluster fails.

Cluster unit

A FortiGate unit operating in a FortiGate HA cluster.

Device failover

Device failover is a basic requirement of any highly available system. Device failover means that if a device fails, a replacement device automatically takes the place of the failed device and continues operating in the same manner as the failed device.

Failover

A FortiGate unit taking over processing network traffic in place of another unit in the cluster that suffered a device failure or a link failure.

Failure

A hardware or software problem that causes a FortiGate unit or a monitored interface to stop processing network traffic.

FGCP

The FortiGate clustering protocol (FGCP) that specifies how the FortiGate units in a cluster communicate to keep the cluster operating.

Full mesh HA

Full mesh HA is a method of removing single points of failure on a network that includes an HA cluster. FortiGate models that support redundant interfaces can be used to create a cluster configuration called full mesh HA. Full mesh HA includes redundant connections between all network components. If any single component or any single connection fails, traffic switches to the redundant component or connection.

HA virtual MAC address

When operating in HA mode, all of the interfaces of the primary unit acquire the same HA virtual MAC address. All communications with the cluster must use this MAC address. The HA virtual MAC address is set according to the group ID.

Heartbeat

Also called FGCP heartbeat or HA heartbeat. The heartbeat constantly communicates HA status and synchronization information to make sure that the cluster is operating properly.

Heartbeat device

An Ethernet network interface in a cluster that is used by the FGCP for heartbeat communications among cluster units.

Heartbeat failover

If an interface functioning as the heartbeat device fails, the heartbeat is transferred to another interface also configured as an HA heartbeat device.

Hello state

In the hello state a cluster unit has powered on in HA mode, is using HA heartbeat interfaces to send hello packets, and is listening on its heartbeat interfaces for hello packets from other FortiGate units. Hello state may appear in HA log messages.

High availability

The ability that a cluster has to maintain a connection when there is a device or link failure by having another unit in the cluster take over the connection, without any loss of connectivity. To achieve high availability, all FortiGate units in the cluster share session and configuration information.

Interface monitoring

You can configure interface monitoring (also called port monitoring) to monitor FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks. If a monitored interface fails or is disconnected from its network the interface leaves the cluster and a link failover occurs. For more information about interface monitoring, see Link failover (port monitoring or interface monitoring).

Link failover

Link failover means that if a monitored interface fails, the cluster reorganizes to re-establish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic.

Load balancing

Also known as active-active HA. All units in the cluster process network traffic. The FGCP employs a technique similar to unicast load balancing. The primary unit interfaces are assigned virtual MAC addresses which are associated on the network with the cluster IP addresses. The primary unit is the only cluster unit to receive packets sent to the cluster. The primary unit can process packets itself, or propagate them to subordinate units according to a load balancing schedule. Communication between the cluster units uses the actual cluster unit MAC addresses.

Monitored interface

An interface that is monitored by a cluster to make sure that it is connected and operating correctly. The cluster monitors the connectivity of this interface for all cluster units. If a monitored interface fails or becomes disconnected from its network, the cluster will compensate.

Primary unit

Also called the primary cluster unit, this cluster unit controls how the cluster operates. The primary unit sends hello packets to all cluster units to synchronize session information, synchronize the cluster configuration, and to synchronize the cluster routing table. The hello packets also confirm for the subordinate units that the primary unit is still functioning.

The primary unit also tracks the status of all subordinate units. When you start a management connection to a cluster, you connect to the primary unit.

In an active-passive cluster, the primary unit processes all network traffic. If a subordinate unit fails, the primary unit updates the cluster configuration database.

In an active-active cluster, the primary unit receives all network traffic and re-directs this traffic to subordinate units. If a subordinate unit fails, the primary unit updates the cluster status and redistributes load balanced traffic to other subordinate units in the cluster.

The FortiGate firmware uses the term master to refer to the primary unit.

Session failover

Session failover means that a cluster maintains active network sessions after a device or link failover. FortiGate HA does not support session failover by default. To enable session failover you must change the HA configuration to select Enable Session Pick-up.

Session pickup

If you enable session pickup for a cluster, if the primary unit fails or a subordinate unit in an active-active cluster fails, all communication sessions with the cluster are maintained or picked up by the cluster after the cluster negotiates to select a new primary unit.

If session pickup is not a requirement of your HA installation, you can disable this option to save processing resources and reduce the network bandwidth used by HA session synchronization. In many cases interrupted sessions will resume on their own after a failover even if session pickup is not enabled. You can also enable session pickup delay to reduce the number of sessions that are synchronized by session pickup.

Standby state

A subordinate unit in an active-passive HA cluster operates in the standby state. In a virtual cluster, a subordinate virtual domain also operates in the standby state. The standby state is actually a hot-standby state because the subordinate unit or subordinate virtual domain is not processing traffic but is monitoring the primary unit session table to take the place of the primary unit or primary virtual domain if a failure occurs.

In an active-active cluster all cluster units operate in a work state.

When standby state appears in HA log messages this usually means that a cluster unit has become a subordinate unit in an active-passive cluster or that a virtual domain has become a subordinate virtual domain.

State synchronization

The part of the FGCP that maintains connections after failover.

Subordinate unit

Also called the subordinate cluster unit, each cluster contains one or more cluster units that are not functioning as the primary unit. Subordinate units are always waiting to become the primary unit. If a subordinate unit does not receive hello packets from the primary unit, it attempts to become the primary unit.

In an active-active cluster, subordinate units keep track of cluster connections, keep their configurations and routing tables synchronized with the primary unit, and process network traffic assigned to them by the primary unit. In an active-passive cluster, subordinate units do not process network traffic. However, active-passive subordinate units do keep track of cluster connections and do keep their configurations and routing tables synchronized with the primary unit.

The FortiGate firmware uses the terms slave and subsidiary unit to refer to a subordinate unit.

Virtual clustering

Virtual clustering is an extension of the FGCP for FortiGate units operating with multiple VDOMS enabled. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a VDOM operating on two different cluster units. You can also operate virtual clustering in active-active mode to use HA load balancing to load balance sessions between cluster units. Alternatively, by distributing VDOM processing between the two cluster units you can also configure virtual clustering to provide load balancing by distributing sessions for different VDOMs to each cluster unit.

Work state

The primary unit in an active-passive HA cluster, a primary virtual domain in a virtual cluster, and all cluster units in an active-active cluster operate in the work state. A cluster unit operating in the work state processes traffic, monitors the status of the other cluster units, and tracks the session table of the cluster.

When work state appears in HA log messages this usually means that a cluster unit has become the primary unit or that a virtual domain has become a primary virtual domain.

HA web-based manager options

Go to **System > Config > HA** to change HA options. You can set the following options to put a FortiGate unit into HA mode. You can also change any of these options while the cluster is operating.

You can configure HA options for a FortiGate unit with virtual domains (VDOMs) enabled by logging into the web-based manager as the global admin administrator and going to **System > Config > HA**.

If already operating in HA mode, go to **System > Config > HA to** display the cluster members list (see Cluster members list).

Go to **System > Config > HA** and select **View HA Statistics** to view statistics about cluster operation. See Viewing HA statistics.

If your cluster uses virtual domains, you are configuring HA virtual clustering. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below and see Virtual clusters on page 1387.

FortiGate HA is compatible with DHCP and PPPoE but care should be taken when configuring a cluster that includes a FortiGate interface configured to get its IP address with DHCP or PPPoE. Fortinet recommends that you turn on DHCP or PPPoE addressing for an interface after the cluster has been configured. If an interface is configured for DHCP or PPPoE, turning on high availability may result in the interface receiving an incorrect address or not being able to connect to the DHCP or PPPoE server correctly.

Mode

Select an HA mode for the cluster or return the FortiGate unit in the cluster to standalone mode. When configuring a cluster, you must set all members of the HA cluster to the same HA mode. You can select **Standalone** (to disable HA), **Active-Passive**, or **Active-Active**.

If virtual domains are enabled you can select **Active-Passive** or **Standalone**.

Device Priority

Optionally set the device priority of the cluster FortiGate unit. Each FortiGate unit in a cluster can have a different device priority. During HA negotiation, the FortiGate unit with the highest device priority usually becomes the primary unit.

In a virtual cluster configuration, each cluster FortiGate unit can have two different device priorities, one for each virtual cluster. During HA negotiation, the FortiGate unit with the highest device priority in a virtual cluster becomes the primary FortiGate unit for that virtual cluster.

Changes to the device priority are not synchronized. You can accept the default device priority when first configuring a cluster.

Reserve Management Port for Cluster Member

You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. Once this management interface is reserved, you can configure a different IP address, administrative access and other interface settings for this interface for each cluster unit. Then by connecting this interface of each cluster unit to your network you can manage each cluster unit separately from a different IP address. See Managing individual cluster units using a reserved management interface.

Group Name

Enter a name to identify the cluster. The maximum length of the group name is 32 characters. The group name must be the same for all cluster units before the cluster units can form a cluster. After a cluster is operating, you can change the group name. The group name change is synchronized to all cluster units.

Password

Enter a password to identify the cluster. The password must be the same for all cluster FortiGate units before the cluster FortiGate units can form a cluster.

Two clusters on the same network must have different passwords.

The password is synchronized to all cluster units in an operating cluster. If you change the password of one cluster unit the change is synchronized to all cluster units.

Enable Session pickup

Select to enable session pickup so that if the primary unit fails, sessions are picked up by the cluster unit that becomes the new primary unit.

You must enable session pickup for session failover protection. If you do not require session failover protection, leaving session pickup disabled may reduce HA CPU usage and reduce HA heartbeat network bandwidth usage. See Session failover (session pick-up).

Port Monitor

Select to enable or disable monitoring FortiGate interfaces to verify the monitored interfaces are functioning properly and are connected to their networks. See Link failover (port monitoring or interface monitoring).

If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster FortiGate unit that still has a connection to the network. This other cluster FortiGate unit becomes the new primary unit.

Port monitoring (also called interface monitoring) is disabled by default. Leave port monitoring disabled until the cluster is operating and then only enable port monitoring for connected interfaces.

You can monitor up to 64 interfaces.

Heartbeat Interface

Select to enable or disable HA heartbeat communication for each interface in the cluster and set the heartbeat interface priority. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface with the lowest hash map order value processes all heartbeat traffic. The web-based manager lists interfaces in alphanumeric order:

- port1
- port2 through 9
- port10

Hash map order sorts interfaces in the following order:

- port1
- port10
- port2 through port9

The default heartbeat interface configuration is different for each FortiGate model. This default configuration usually sets the priority of two heartbeat interfaces to 50. You can accept the default heartbeat interface configuration or change it as required.

The heartbeat interface priority range is 0 to 512. The default priority when you select a new heartbeat interface is 0.

You must select at least one heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. See HA heartbeat and communication between cluster units.

You can select up to 8 heartbeat interfaces. This limit only applies to units with more than 8 physical interfaces.

VDOM partitioning

If you are configuring virtual clustering, you can set the virtual domains to be in virtual cluster 1 and the virtual domains to be in virtual cluster 2. The root virtual domain must always be in virtual cluster 1.

FGCP high availability best practices

Fortinet suggests the following practices related to high availability:

- Use Active-Active HA to distribute TCP and UTM sessions among multiple cluster units. An active-active cluster may have higher throughput than a standalone FortiGate unit or than an active-passive cluster.
- Use a different host name on each FortiGate unit when configuring an HA cluster. Fewer steps are required to add host names to each cluster unit before configuring HA and forming a cluster.
- Consider adding an Alias to the interfaces used for the HA heartbeat so that you always get a reminder about what these interfaces are being used for.
- Enabling `load-balance-all` can increase device and network load since more traffic is load-balanced. This may be appropriate for use in a deployment using the firewall capabilities of the FortiGate unit and IPS but no other content inspection.
- An advantage of using session pickup is that non-content inspection sessions will be picked up by the new primary unit after a failover. The disadvantage is that the cluster generates more heartbeat traffic to support session pickup as a larger portion of the session table must be synchronized. Session pickup should be configured only when required and is not recommended for use with SOHO FortiGate models. Session pickup should only be used if the primary heartbeat link is dedicated (otherwise the additional HA heartbeat traffic could affect network performance).
- If session pickup is not selected, after a device or link failover all sessions are briefly interrupted and must be re-established at the application level after the cluster renegotiates. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Users downloading large files may have to restart their download after a failover. Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.

- If you need to enable session pickup, consider enabling session pickup delay to improve performance by reducing the number of sessions that are synchronized.
- Consider using the `session-sync-dev` option to move session synchronization traffic off the HA heartbeat link to one or more dedicated session synchronization interfaces.
- To avoid unpredictable results, when you connect a switch to multiple redundant or aggregate interfaces in an active-passive cluster you should configure separate redundant or aggregate interfaces on the switch; one for each cluster unit.
- Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. Alert messages about cluster failovers may help find and diagnose network problems quickly and efficiently.

Heartbeat interfaces

Fortinet suggests the following practices related to heartbeat interfaces:

Do not use a FortiGate switch port for the HA heartbeat traffic. This configuration is not supported.

- For clusters of two FortiGate units, as much as possible, heartbeat interfaces should be directly connected using patch cables (without involving other network equipment such as switches). If switches have to be used they should not be used for other network traffic that could flood the switches and cause heartbeat delays.
  - If you cannot use a dedicated switch, the use of a dedicated VLAN can help limit the broadcast domain to protect the heartbeat traffic and the bandwidth it creates.
- For clusters of three or four FortiGate units, use switches to connect heartbeat interfaces. The corresponding heartbeat interface of each FortiGate unit in the cluster must be connected to the same switch. For improved redundancy use a different switch for each heartbeat interface. In that way if the switch connecting one of the heartbeat interfaces fails or is unplugged, heartbeat traffic can continue on the other heartbeat interfaces and switch.
- Isolate heartbeat interfaces from user networks. Heartbeat packets contain sensitive cluster configuration information and can consume a considerable amount of network bandwidth. If the cluster consists of two FortiGate units, connect the heartbeat interfaces directly using a crossover cable or a regular Ethernet cable. For clusters with more than two units, connect heartbeat interfaces to a separate switch that is not connected to any network.
- If heartbeat traffic cannot be isolated from user networks, enable heartbeat message encryption and authentication to protect cluster information. See Enabling or disabling HA heartbeat encryption and authentication.
- Configure and connect redundant heartbeat interfaces so that if one heartbeat interface fails or becomes disconnected, HA heartbeat traffic can continue to be transmitted using the backup heartbeat interface. If heartbeat communication fails, all cluster members will think they are the primary unit resulting in multiple devices on the network with the same IP addresses and MAC addresses (condition referred to as *Split Brain*) and communication will be disrupted until heartbeat communication can be reestablished.
- Do not monitor dedicated heartbeat interfaces; monitor those interfaces whose failure should trigger a device failover.
- Where possible at least one heartbeat interface should not be connected to an NPx processor to avoid NPx-related problems from affecting heartbeat traffic.

Interface monitoring (port monitoring)

Fortinet suggests the following practices related to interface monitoring (also called port monitoring):

- Wait until a cluster is up and running and all interfaces are connected before enabling interface monitoring. A monitored interface can easily become disconnected during initial setup and cause failovers to occur before the cluster is fully configured and tested.
- Monitor interfaces connected to networks that process high priority traffic so that the cluster maintains connections to these networks if a failure occurs.
- Avoid configuring interface monitoring for all interfaces.
- Supplement interface monitoring with remote link failover. Configure remote link failover to maintain packet flow if a link not directly connected to a cluster unit (for example, between a switch connected to a cluster interface and the network) fails. See Remote link failover.

FGCP HA terminology

The following HA-specific terms are used in this document.

Cluster

A group of FortiGate units that act as a single virtual FortiGate unit to maintain connectivity even if one of the FortiGate units in the cluster fails.

Cluster unit

A FortiGate unit operating in a FortiGate HA cluster.

Device failover

Device failover is a basic requirement of any highly available system. Device failover means that if a device fails, a replacement device automatically takes the place of the failed device and continues operating in the same manner as the failed device.

Failover

A FortiGate unit taking over processing network traffic in place of another unit in the cluster that suffered a device failure or a link failure.

Failure

A hardware or software problem that causes a FortiGate unit or a monitored interface to stop processing network traffic.

FGCP

The FortiGate clustering protocol (FGCP) that specifies how the FortiGate units in a cluster communicate to keep the cluster operating.

Full mesh HA

Full mesh HA is a method of removing single points of failure on a network that includes an HA cluster. FortiGate models that support redundant interfaces can be used to create a cluster configuration called full mesh HA. Full mesh HA includes redundant connections between all network components. If any single component or any single connection fails, traffic switches to the redundant component or connection.

HA virtual MAC address

When operating in HA mode, all of the interfaces of the primary unit acquire the same HA virtual MAC address. All communications with the cluster must use this MAC address. The HA virtual MAC address is set according to the group ID.

Heartbeat

Also called FGCP heartbeat or HA heartbeat. The heartbeat constantly communicates HA status and synchronization information to make sure that the cluster is operating properly.

Heartbeat device

An Ethernet network interface in a cluster that is used by the FGCP for heartbeat communications among cluster units.

Heartbeat failover

If an interface functioning as the heartbeat device fails, the heartbeat is transferred to another interface also configured as an HA heartbeat device.

Hello state

In the hello state a cluster unit has powered on in HA mode, is using HA heartbeat interfaces to send hello packets, and is listening on its heartbeat interfaces for hello packets from other FortiGate units. Hello state may appear in HA log messages.

High availability

The ability that a cluster has to maintain a connection when there is a device or link failure by having another unit in the cluster take over the connection, without any loss of connectivity. To achieve high availability, all FortiGate units in the cluster share session and configuration information.

Interface monitoring

You can configure interface monitoring (also called port monitoring) to monitor FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks. If a monitored interface fails or is disconnected from its network the interface leaves the cluster and a link failover occurs. For more information about interface monitoring, see Link failover (port monitoring or interface monitoring).

Link failover

Link failover means that if a monitored interface fails, the cluster reorganizes to re-establish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic.

Load balancing

Also known as active-active HA. All units in the cluster process network traffic. The FGCP employs a technique similar to unicast load balancing. The primary unit interfaces are assigned virtual MAC addresses which are

associated on the network with the cluster IP addresses. The primary unit is the only cluster unit to receive packets sent to the cluster. The primary unit can process packets itself, or propagate them to subordinate units according to a load balancing schedule. Communication between the cluster units uses the actual cluster unit MAC addresses.

Monitored interface

An interface that is monitored by a cluster to make sure that it is connected and operating correctly. The cluster monitors the connectivity of this interface for all cluster units. If a monitored interface fails or becomes disconnected from its network, the cluster will compensate.

Primary unit

Also called the primary cluster unit, this cluster unit controls how the cluster operates. The primary unit sends hello packets to all cluster units to synchronize session information, synchronize the cluster configuration, and to synchronize the cluster routing table. The hello packets also confirm for the subordinate units that the primary unit is still functioning.

The primary unit also tracks the status of all subordinate units. When you start a management connection to a cluster, you connect to the primary unit.

In an active-passive cluster, the primary unit processes all network traffic. If a subordinate unit fails, the primary unit updates the cluster configuration database.

In an active-active cluster, the primary unit receives all network traffic and re-directs this traffic to subordinate units. If a subordinate unit fails, the primary unit updates the cluster status and redistributes load balanced traffic to other subordinate units in the cluster.

The FortiGate firmware uses the term master to refer to the primary unit.

Session failover

Session failover means that a cluster maintains active network sessions after a device or link failover. FortiGate HA does not support session failover by default. To enable session failover you must change the HA configuration to select Enable Session Pick-up.

Session pickup

If you enable session pickup for a cluster, if the primary unit fails or a subordinate unit in an active-active cluster fails, all communication sessions with the cluster are maintained or picked up by the cluster after the cluster negotiates to select a new primary unit.

If session pickup is not a requirement of your HA installation, you can disable this option to save processing resources and reduce the network bandwidth used by HA session synchronization. In many cases interrupted sessions will resume on their own after a failover even if session pickup is not enabled. You can also enable session pickup delay to reduce the number of sessions that are synchronized by session pickup.

Standby state

A subordinate unit in an active-passive HA cluster operates in the standby state. In a virtual cluster, a subordinate virtual domain also operates in the standby state. The standby state is actually a hot-standby state because the

subordinate unit or subordinate virtual domain is not processing traffic but is monitoring the primary unit session table to take the place of the primary unit or primary virtual domain if a failure occurs.

In an active-active cluster all cluster units operate in a work state.

When standby state appears in HA log messages this usually means that a cluster unit has become a subordinate unit in an active-passive cluster or that a virtual domain has become a subordinate virtual domain.

State synchronization

The part of the FGCP that maintains connections after failover.

Subordinate unit

Also called the subordinate cluster unit, each cluster contains one or more cluster units that are not functioning as the primary unit. Subordinate units are always waiting to become the primary unit. If a subordinate unit does not receive hello packets from the primary unit, it attempts to become the primary unit.

In an active-active cluster, subordinate units keep track of cluster connections, keep their configurations and routing tables synchronized with the primary unit, and process network traffic assigned to them by the primary unit. In an active-passive cluster, subordinate units do not process network traffic. However, active-passive subordinate units do keep track of cluster connections and do keep their configurations and routing tables synchronized with the primary unit.

The FortiGate firmware uses the terms slave and subsidiary unit to refer to a subordinate unit.

Virtual clustering

Virtual clustering is an extension of the FGCP for FortiGate units operating with multiple VDOMS enabled. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a VDOM operating on two different cluster units. You can also operate virtual clustering in active-active mode to use HA load balancing to load balance sessions between cluster units. Alternatively, by distributing VDOM processing between the two cluster units you can also configure virtual clustering to provide load balancing by distributing sessions for different VDOMs to each cluster unit.

Work state

The primary unit in an active-passive HA cluster, a primary virtual domain in a virtual cluster, and all cluster units in an active-active cluster operate in the work state. A cluster unit operating in the work state processes traffic, monitors the status of the other cluster units, and tracks the session table of the cluster.

When work state appears in HA log messages this usually means that a cluster unit has become the primary unit or that a virtual domain has become a primary virtual domain.

HA GUI options

Go to **System > Config > HA** to change HA options. You can set the following options to put a FortiGate unit into HA mode. You can also change any of these options while the cluster is operating.

You can configure HA options for a FortiGate unit with virtual domains (VDOMs) enabled by logging into the web-based manager as the global admin administrator and going to **System > Config > HA**.

If already operating in HA mode, go to **System > Config > HA to** display the cluster members list (see Cluster members list).

Go to **System > Config > HA** and select **View HA Statistics** to view statistics about cluster operation. See Viewing HA statistics.

If your cluster uses virtual domains, you are configuring HA virtual clustering. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below and see Virtual clusters on page 1387.

FortiGate HA is compatible with DHCP and PPPoE but care should be taken when configuring a cluster that includes a FortiGate interface configured to get its IP address with DHCP or PPPoE. Fortinet recommends that you turn on DHCP or PPPoE addressing for an interface after the cluster has been configured. If an interface is configured for DHCP or PPPoE, turning on high availability may result in the interface receiving an incorrect address or not being able to connect to the DHCP or PPPoE server correctly.

Mode

Select an HA mode for the cluster or return the FortiGate unit in the cluster to standalone mode. When configuring a cluster, you must set all members of the HA cluster to the same HA mode. You can select **Standalone** (to disable HA), **Active-Passive**, or **Active-Active**.

If virtual domains are enabled you can select **Active-Passive** or **Standalone**.

Device Priority

Optionally set the device priority of the cluster FortiGate unit. Each FortiGate unit in a cluster can have a different device priority. During HA negotiation, the FortiGate unit with the highest device priority usually becomes the primary unit.

In a virtual cluster configuration, each cluster FortiGate unit can have two different device priorities, one for each virtual cluster. During HA negotiation, the FortiGate unit with the highest device priority in a virtual cluster becomes the primary FortiGate unit for that virtual cluster.

Changes to the device priority are not synchronized. You can accept the default device priority when first configuring a cluster.

Reserve Management Port for Cluster Member

You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. Once this management interface is reserved, you can configure a different IP address, administrative access and other interface settings for this interface for each cluster unit. Then by connecting this interface of each cluster unit to your network you can manage each cluster unit separately from a different IP address. See Managing individual cluster units using a reserved management interface.

Do NOT Synchronize Management VDOM Configuration

This options appears if you have enabled multiple VDOMS and set a VDOM other than the root VDOM to be the management VDOM. You can select this option to prevent the management VDOM configuration from being synchronized between cluster units in the virtual cluster. This allows you to add an interface to the VDOM in each cluster unit and then to give the Interfacea different IP address in each cluster unit, allowing you to manage eachc cluster unit separately.

You can also enable this feature using the following command:

```
config system ha
   set standalone-mgmt-vdom enable
end
```

Group Name

Enter a name to identify the cluster. The maximum length of the group name is 32 characters. The group name must be the same for all cluster units before the cluster units can form a cluster. After a cluster is operating, you can change the group name. The group name change is synchronized to all cluster units.

Password

Enter a password to identify the cluster. The password must be the same for all cluster FortiGate units before the cluster FortiGate units can form a cluster.

Two clusters on the same network must have different passwords.

The password is synchronized to all cluster units in an operating cluster. If you change the password of one cluster unit the change is synchronized to all cluster units.

Enable Session pickup

Select to enable session pickup so that if the primary unit fails, sessions are picked up by the cluster unit that becomes the new primary unit.

You must enable session pickup for session failover protection. If you do not require session failover protection, leaving session pickup disabled may reduce HA CPU usage and reduce HA heartbeat network bandwidth usage. See Session failover (session pick-up).

Port Monitor

Select to enable or disable monitoring FortiGate interfaces to verify the monitored interfaces are functioning properly and are connected to their networks. See Link failover (port monitoring or interface monitoring).

If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster FortiGate unit that still has a connection to the network. This other cluster FortiGate unit becomes the new primary unit.

Port monitoring (also called interface monitoring) is disabled by default. Leave port monitoring disabled until the cluster is operating and then only enable port monitoring for connected interfaces.

You can monitor up to 64 interfaces.

Heartbeat Interface

Select to enable or disable HA heartbeat communication for each interface in the cluster and set the heartbeat interface priority. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface with the lowest hash map order value processes all heartbeat traffic. The web-based manager lists interfaces in alphanumeric order:

- port1
- port2 through 9
- port10

Hash map order sorts interfaces in the following order:

- port1
- port10
- port2 through port9

The default heartbeat interface configuration is different for each FortiGate model. This default configuration usually sets the priority of two heartbeat interfaces to 50. You can accept the default heartbeat interface configuration or change it as required.

The heartbeat interface priority range is 0 to 512. The default priority when you select a new heartbeat interface is 0.

You must select at least one heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. See HA heartbeat and communication between cluster units.

You can select up to 8 heartbeat interfaces. This limit only applies to units with more than 8 physical interfaces.

VDOM partitioning

If you are configuring virtual clustering, you can set the virtual domains to be in virtual cluster 1 and the virtual domains to be in virtual cluster 2. The root virtual domain must always be in virtual cluster 1.

FGCP configuration examples and troubleshooting

This chapter contains general procedures and descriptions as well as detailed configuration examples that describe how to configure FortiGate HA clusters.

The examples in this chapter include example values only. In most cases you will substitute your own values. The examples in this chapter also do not contain detailed descriptions of configuration parameter

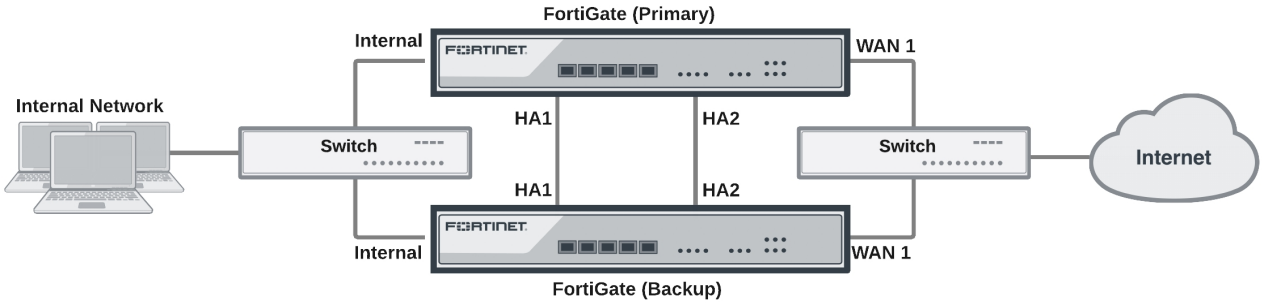
About the examples in this chapter

The procedures in this chapter describe some of many possible sequences of steps for configuring HA clustering. As you become more experienced with FortiOS HA you may choose to use a different sequence of configuration steps.

For simplicity, many of these procedures assume that you are starting with new FortiGate units set to the factory default configuration. However, starting from the default configuration is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

How to set up FGCP clustering (recommended steps)

This example describes how to enhance the reliability of a network protected by a FortiGate unit by adding a second FortiGate unit to create a FortiGate Clustering Protocol (FGCP) High Availability cluster.



The FortiGate already on the network will be configured to become the primary unit by increasing its device priority and enabling override. The new FortiGate will be prepared by setting it to factory defaults to wipe any configuration changes. Then it will be licensed, configured for HA, and then connected to the FortiGate already on the network. The new FortiGate becomes the backup unit and its configuration is overwritten by the primary unit.

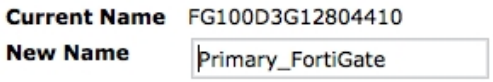
The recipe contains instructions for both the GUI and the CLI, with some parts of the configuration requiring use of the CLI.

Before you start the FortiGates should be running the same FortiOS firmware version and interfaces should not be configured to get their addresses from DHCP or PPPoE.

1. Configuring the primary FortiGate

If the FortiGates in the cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

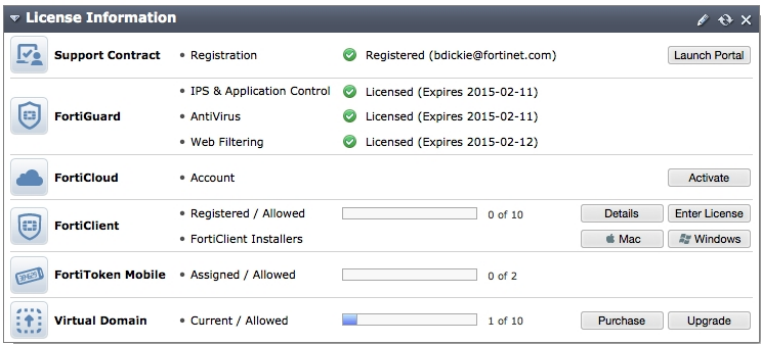
Connect to the primary FortiGate and go to **System > Dashboard > Status** and locate the **System Information** widget. Change the unit's **Host Name** to identify it as the primary FortiGate.



You can also enter this CLI command:

```
config system global
  set hostname Primary_FortiGate
end
```

If you have not already done so, register the primary FortiGate and apply licenses to it before setting up the cluster. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate. FortiToken licenses can be added at any time because they are synchronized to all cluster members.



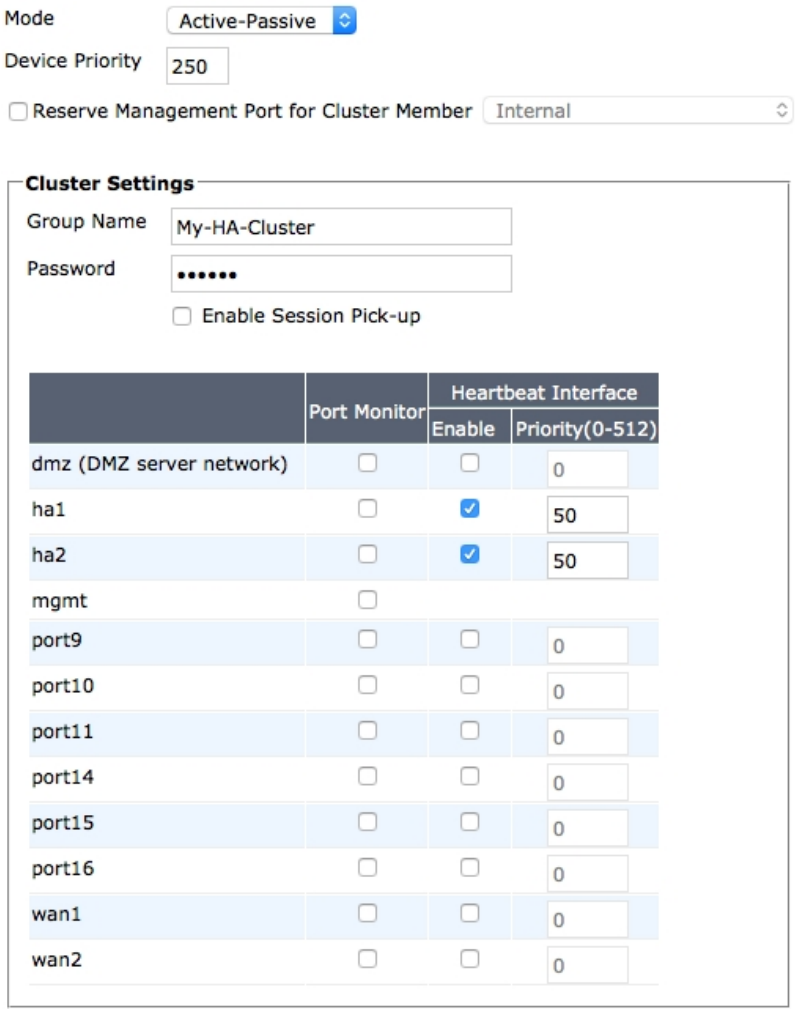
Enter this CLI command to set the HA mode to active-passive, set a group name and password, increase the device priority to a higher value (for example, 250) and enable override.

```
config system ha
  set mode a-p
  set group-name My-HA-Cluster
  set password
  set priority 250
  set override enable
  set hbdev ha1 50 ha2 50
end
```

Enabling override and increasing the device priority means this unit should always become the primary unit.

This command also selects ha1 and ha2 to be the heartbeat interfaces and sets their priorities to 50.

You can also use the GUI to configure most of these settings.



Override can only be enabled from the CLI.

```
config system ha
   set override enable
end
```

The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as FGCP negotiation takes place and the MAC addresses of the FortiGate unit are changed to HA virtual MAC addresses. These virtual MAC addresses are used for failover. The actual virtual MAC address assigned to each FortiGate interface depends on the HA group ID. Since this example does not involved changing the HA group ID, the FortiGate unit's interfaces will have the following MAC addresses: 00:09:0f:09:00:00, 00:09:0f:09:00:01, 00:09:0f:09:00:02 and so on.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You can usually delete the arp table from a command prompt using a command similar to `arp -d`.

To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) command to view the virtual MAC address of any FortiGate unit interface. Depending on the FortiGate model, the output from this command could include lines similar to the following:

```
Current_HWaddr: 00:09:0f:09:00:00
Permanent_HWaddr 02:09:0f:78:18:c9
```

2. Configuring the backup FortiGate

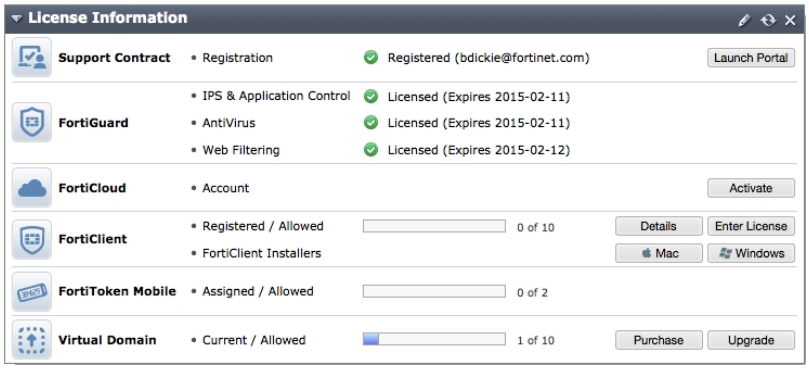
Enter this command to reset the new FortiGate to factory default settings.

```
execute factoryreset
```

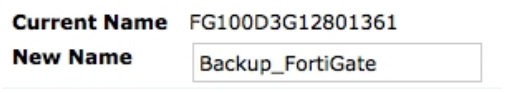
You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all it is recommended to set it back to factory defaults to reduce the chance of synchronization problems.

Change the firmware running on the new FortiGate to be the same version as is running on the primary unit.

Register the backup FortiGate and apply licenses to it before adding it to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). FortiToken licenses can be added at any time because they are synchronized to all cluster members.



Go to **System > Dashboard > Status** and change the unit's **Host Name** to identify it as the backup FortiGate.

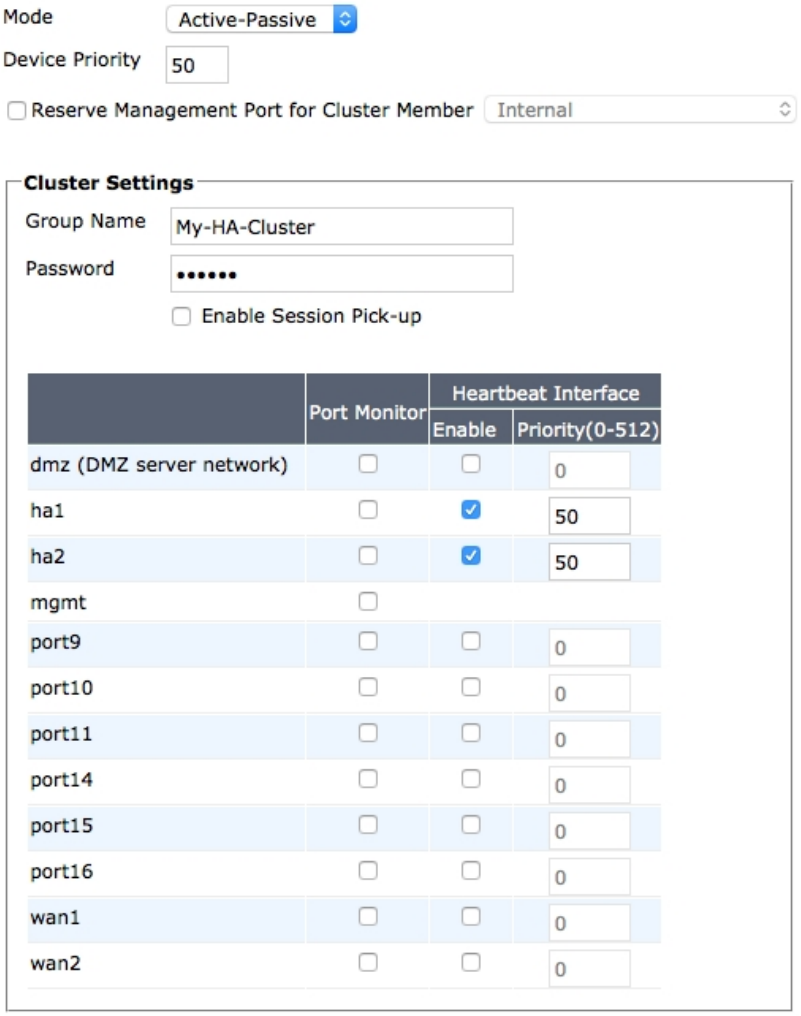


You can also enter this CLI command:

```
config system global
   set hostname Backup_FortiGate
end
```

Duplicate the primary unit HA settings, except set the device priority to a lower value and do not enable override.

You can configure all of these settings from the GUI.



You can also enter this CLI command:

```
config system ha
   set mode a-p
   set group-name My-HA-Cluster
   set password
   set priority 50
   set hbdev ha1 50 ha2 50
end
```

3. Connecting the cluster

Connect the HA cluster as shown in the initial diagram. Making these connections will disrupt network traffic as you disconnect and re-connect cables.

When connected the primary and backup FortiGates find each other and negotiate to form an HA cluster. The Primary unit synchronizes its configuration with the backup FortiGate. Forming the cluster happens automatically with minimal or no disruption to network traffic.

4. Checking cluster operation and disabling override

Check the cluster synchronization status to make sure the primary and backup units have the same configuration. Log into the primary unit CLI and enter this command:

```
diag sys ha cluster-csum
```

The CLI lists all members' checksums. If both cluster units have identical checksums you can be sure that their configurations are synchronized. If the checksums are different wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical contact Fortinet support to help troubleshoot the problem.

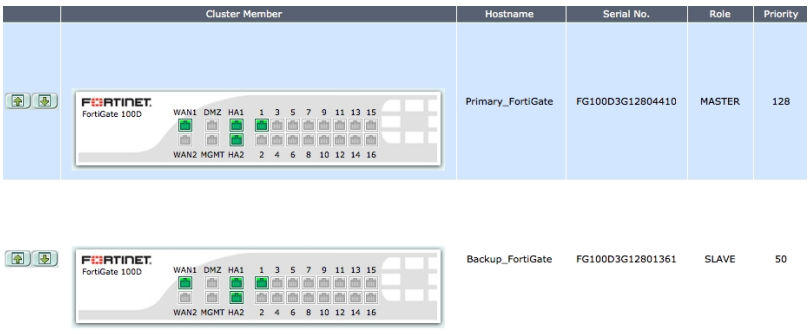
Disable override on the primary unit (recommended).

```
config system ha
    set override disable
end
```

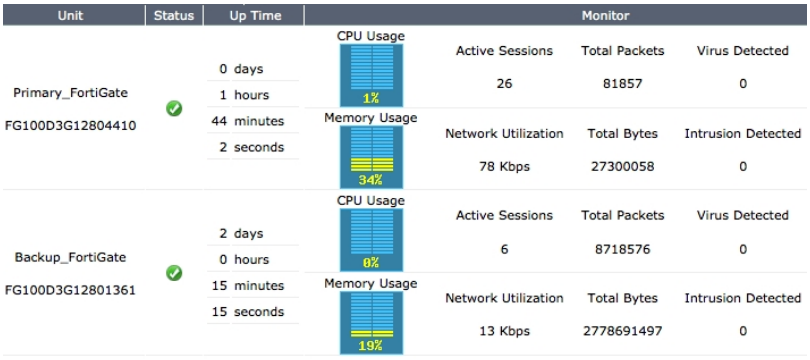
The HA cluster dynamically responds to network conditions. If you keep override enabled the same FortiGate will always be the primary FortiGate. Because of this, however; the cluster may negotiate more often potentially disrupting traffic.

If you disable override it is more likely that the new FortiGate unit could become the primary unit. Disabling override is recommended unless its important that the same FortiGate remains the primary unit.

Connect to the primary FortiGate GUI and go to **System > Config > HA** to view the cluster information.



Select **View HA Statistics** for more information on how the cluster is operating and processing traffic.



5. Results

Normally, traffic should now be flowing through the primary FortiGate. However, if the primary FortiGate is unavailable, traffic should failover and the backup FortiGate will be used. Failover will also cause the primary and backup FortiGates to reverse roles, even when both FortiGates are available again.

To test this, ping the IP address 8.8.8.8 using a PC on the internal network. After a moment, power off the primary FortiGate.

```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

You will see a momentary pause in the Ping results, until traffic diverts to the backup FortiGate, allowing the Ping traffic to continue.

If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

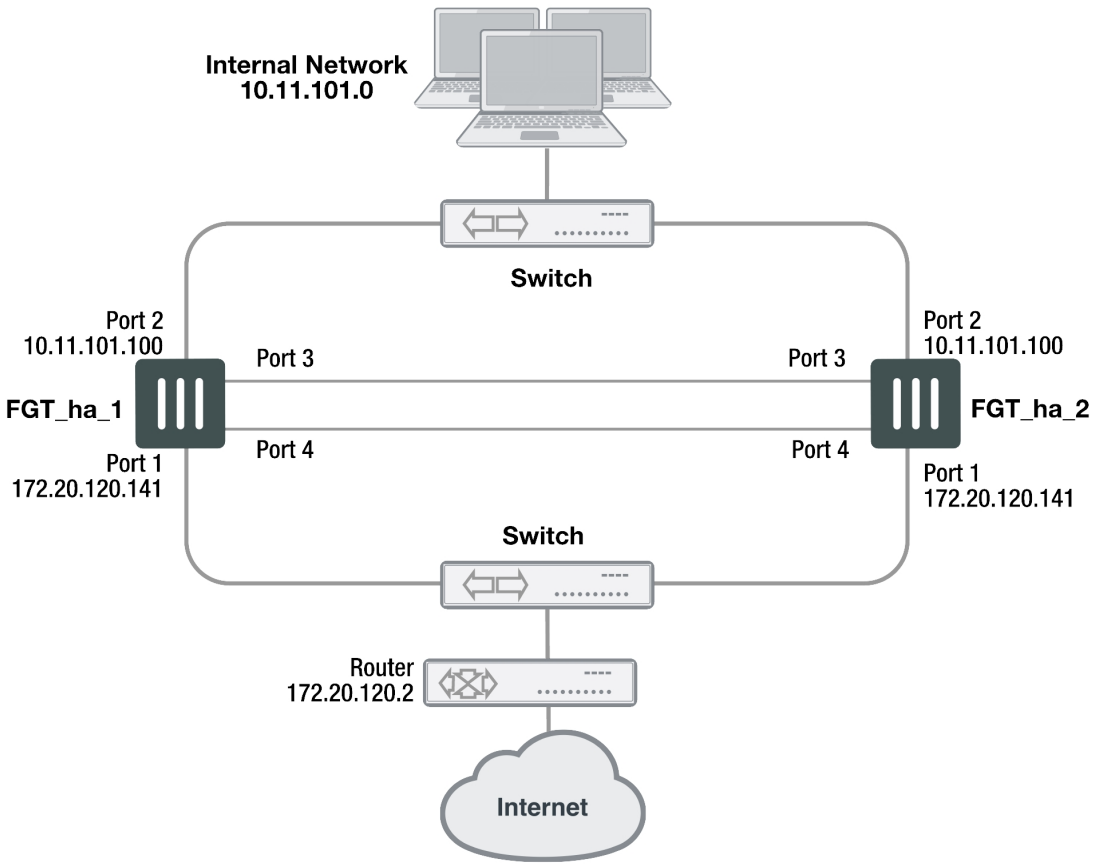
Setting up two new FortiGates as an FGCP cluster

This section describes a simple HA network topology that includes an HA cluster of two FortiGate units in NAT/Route mode installed between an internal network and the Internet. The example uses a generic FortiGate unit with four interfaces named port1, port2, port3 and port4.

Example NAT/Route mode HA network topology

The figure below shows a typical FortiGate HA cluster consisting of two FortiGate units (FGT_ha_1 and FGT_ha_2) connected to the same internal (port2) and external (port1) networks.

Example NAT/Route mode HA network topology



Port3 and port4 are used as the heartbeat interfaces. Because the cluster consists of two FortiGate units, you can make the connections between the heartbeat interfaces using crossover cables. You could also use switches and regular ethernet cables.

General configuration steps

The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate units are running the same FortiOS firmware build and are set to the factory default configuration.

General configuration steps

1. Apply licenses to the FortiGate units to become the cluster.
2. Configure the FortiGate units for HA operation.
   - Optionally change each unit's host name.
   - Configure HA.
2. Connect the cluster to the network.
3. Confirm that the cluster units are operating as a cluster and add basic configuration settings to the cluster.

- View cluster status from the web-based manager or CLI.
- Add a password for the admin administrative account.
- Change the IP addresses and netmasks of the internal and external interfaces.
- Add a default route.

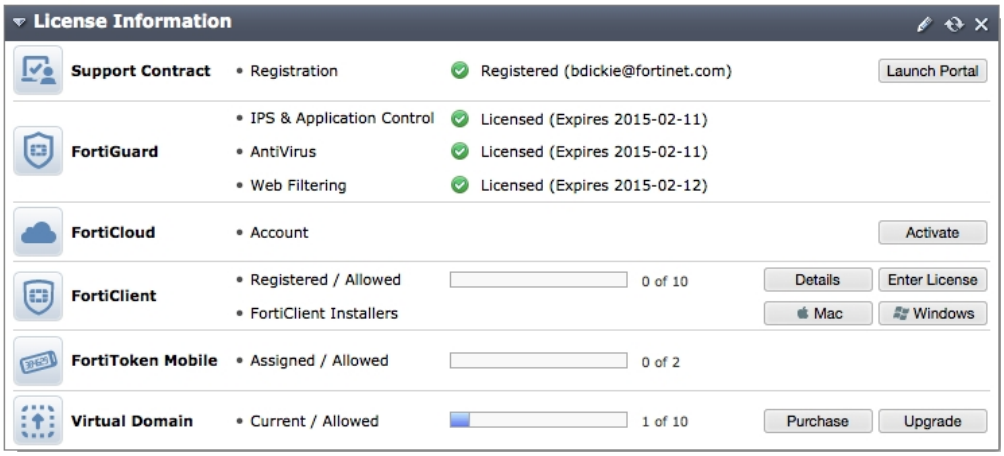
Configuring a NAT/Route mode active-passive cluster of two FortiGate units - web-based manager

Use the following procedures to configure two FortiGate units for NAT/Route HA operation using the web-based manager. These procedures assume you are starting with two FortiGate units with factory default settings.

Give each cluster unit a unique host name to make the individual units easier to identify when they are part of a functioning cluster. The default host name is the FortiGate serial number. You may want to change this host name to something more meaningful for your network.

To configure the first FortiGate unit (host name FGT_ha_1)

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget beside **Host Name**, select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Select **OK**.
6. Go to **System > Config > HA** and change the following settings:

Mode	Active-Passive
Group Name	example1.com
Password	HA_pass_1

This is the minimum recommended configuration for an active-passive HA cluster. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each unit in the cluster.

7. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:
   - port1 interface virtual MAC: `00-09-0f-09-00-00`
   - port2 interface virtual MAC: `00-09-0f-09-00-01`
   - port3 interface virtual MAC: `00-09-0f-09-00-02`
   - port4 interface virtual MAC: `00-09-0f-09-00-03`

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

   To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`MAC`) and the port1 permanent MAC address (`Permanent_HWaddr`):

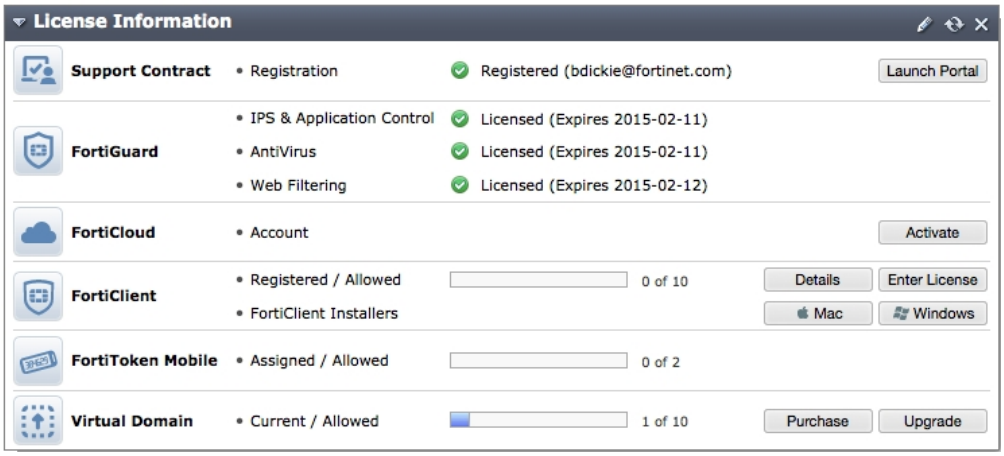
```
get hardware nic port1
.
.
.
Current_HWaddr:  00:09:0f:09:00:00
Permanent_HWaddr  02:09:0f:78:18:c9
.
.
.
```

10. Power off the first FortiGate unit (FGT_ha_1).

Note the details and format of the output of the `get hardware nic` command are specific to the interface hardware. Different FortiGate models and even different interfaces in the same FortiGate unit may have different output.

To configure the second FortiGate unit (host name FGT_ha_2)

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
3. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_2

4. Select **OK**.
5. Go to **System > Config > HA** and change the following settings:

Mode	Active-Passive
Group Name	example1.com
Password	HA_pass_1

6. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces.

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.
7. Power off the second FortiGate unit.

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
3. Connect the port3 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation

occurs with no user intervention and normally takes less than a minute.

When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster.

Once the cluster is operating, because configuration changes are synchronized to all cluster units, configuring the cluster is the same as configuring an individual FortiGate unit. You could have performed the following configuration steps separately on each FortiGate unit before you connected them to form a cluster.

1. Start Internet Explorer and browse to the address https://192.168.1.99 (remember to include the “s” in https://).
   The FortiGate Login is displayed.
2. Type `admin` in the **Name** field and select Login.
   The FortiGate dashboard is displayed.
   The **System Information** dashboard widget shows the **Cluster Name** (example1.com) and the host names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.
3. Go to **System > Config > HA** to view the cluster members list.
   The list shows both cluster units, their host names, their roles in the cluster, and their device priorities. You can use this list to confirm that the cluster is operating normally. For example, if the list shows only one cluster unit then the other unit has left the cluster for some reason.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard do not display information for both cluster units, the FortiGate units are not functioning as a cluster. See Setting up two new FortiGates as an FGCP cluster on page 1319 to troubleshoot the cluster.

To add basic configuration settings to the cluster

Use the following steps to configure the cluster to connect to its network. The following are example configuration steps only and do not represent all of the steps required to configure the cluster for a given network.

1. Log into the cluster web-based manager.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.
5. Select **OK**.
6. Go to **System > Network > Interfaces**.
7. Edit the **port2** interface and change **IP/Netmask** to 10.11.101.100/24.
8. Select **OK**.

After changing the IP address of the port1 interface you may have to change the IP address of your management computer and then reconnect to the port1 interface using the 172.20.120.141 IP address.

9. Edit the **port1** interface and change **IP/Netmask** to 172.20.120.141/24.
10. Select **OK**.
11. Go to **Router > Static > Static Routes**.
12. Change the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	port1
Distance	10

13. Select **OK**.

Configuring a NAT/Route mode active-passive cluster of two FortiGate units - CLI

Use the following procedures to configure two FortiGate units for NAT/Route HA operation using the FortiGate CLI. These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the first FortiGate unit (host name FGT_ha_1)

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal (or any terminal emulation program), enter a name for the connection, and select **OK**.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select **OK**.
5. Select the following port settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press **Enter** to connect to the FortiGate CLI.
   The FortiGate unit CLI login prompt appears.
   If the prompt does not appear, press Enter. If it still does not appear, power off your FortiGate unit and power it back on. If you are connected, at this stage you will see startup messages that will confirm you are connected. The login prompt will appear after the startup has completed.
7. Type `admin` and press **Enter** twice.
8. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
9. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.

FortiToken licenses can be added at any time because they are synchronized to all cluster members.

10. Change the host name for this FortiGate unit.

```
config system global
   set hostname FGT_ha_1
end
```

11. Configure HA settings.

```
config system ha
   set mode a-p
   set group-name example1.com
   set password HA_pass_1
end
```

The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose network connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port2 interface virtual MAC: `00-09-0f-09-00-01`
- port3 interface virtual MAC: `00-09-0f-09-00-02`
- port4 interface virtual MAC: `00-09-0f-09-00-03`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`MAC`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
Current_HAaddr    00:09:0f:09:00:00
Permanent_HWaddr  02:09:0f:78:18:c9
.
.
.
```

10. Display the HA configuration (optional).

```
get system ha
   group-id : 0
   group-name : example1.com
   mode : a-p
   password : *
   hbdev : "port3" 50 "port4" 50
   session-sync-dev    :
   route-ttl : 10
   route-wait : 0
   route-hold : 10
   sync-config : enable
   encryption : disable
   authentication : disable
```

```
hb-interval : 2
hb-lost-threshold : 20
helo-holddown : 20
arps : 5
arps-interval : 8
session-pickup : disable
update-all-session-timer: disable
session-sync-daemon-number: 1
link-failed-signal : disable
uninterruptible-upgrade: enable
ha-mgmt-status : disable
ha-eth-type : 8890
hc-eth-type : 8891
l2ep-eth-type : 8893
ha-uptime-diff-margin: 300
vcluster2 : disable
vcluster-id : 1
override : disable
priority : 128
slave-switch-standby: disable
minimum-worker-threshold: 1
monitor :
pingserver-monitor-interface:
pingserver-failover-threshold: 0
pingserver-slave-force-reset: enable
pingserver-flip-timeout: 60
vdom : "root"
```

11. Power off the FortiGate unit.

To configure the second FortiGate unit (host name FGT_ha_2)

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal, enter a name for the connection, and select **OK**.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select **OK**.
5. Select the following port settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press **Enter** to connect to the FortiGate CLI.
   The FortiGate unit CLI login prompt appears.
7. Type `admin` and press **Enter** twice.

8. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activationand **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
9. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
10. Change the host name for this FortiGate unit.

```
config system global
   set hostname FGT_ha_2
end
```

11. Configure HA settings.

```
config system ha
   set mode a-p
   set group-name example1.com
   set password HA_pass_1
end
```

   The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose network connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces.

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

12. Display the HA configuration (optional).

```
get system ha
   group-id : 0
   group-name : example1.com
   mode : a-p
   password : *
   hbdev : "port3" 50 "port4" 50
   session-sync-dev    :
   route-ttl : 10
   route-wait : 0
   route-hold : 10
   sync-config : enable
   encryption : disable
   authentication : disable
   hb-interval : 2
   hb-lost-threshold : 20
   helo-holddown : 20
   arps : 5
   arps-interval : 8
   session-pickup : disable
   update-all-session-timer: disable
   session-sync-daemon-number: 1
   link-failed-signal : disable
   uninterruptible-upgrade: enable
   ha-mgmt-status : disable
   ha-eth-type : 8890
   hc-eth-type : 8891
   l2ep-eth-type : 8893
   ha-uptime-diff-margin: 300
   vcluster2 : disable
   vcluster-id : 1
```

```
override : disable
priority : 128
slave-switch-standby: disable
minimum-worker-threshold: 1
monitor :
pingserver-monitor-interface:
pingserver-failover-threshold: 0
pingserver-slave-force-reset: enable
pingserver-flip-timeout: 60
vdom : "root"
```

13. Power off the FortiGate unit.

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
3. Connect the port3 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.

   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view cluster status from the CLI.

1. Determine which cluster unit is the primary unit.
   - Use the null-modem cable and serial connection to re-connect to the CLI of one of the cluster units.
   - Enter the command `get system status`.
   - If the command output includes `Current HA mode: a-p, master`, the cluster units are operating as a cluster and you have connected to the primary unit. Continue with Step "Setting up two new FortiGates as an FGCP cluster" on page 1319.
   - If the command output includes `Current HA mode: a-p, backup`, you have connected to a subordinate unit. Connect the null-modem cable to the other cluster unit, which should be the primary unit and continue with Step 2.

If the command output includes `Current HA mode: standalone`, the cluster unit is not operating in HA mode and you should review your HA configuration.

2. Enter the following command to confirm the HA configuration of the cluster:

```
get system ha status
   Model: XXXXX
   Mode: a-p
   Group: 0
   Debug: 0
   ses_pickup: disable
```

```
Master:128 FGT_ha_2 FG600B3908600825 0
Slave :128 FGT_ha_1 FG600B3908600705 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG600B3908600825
Slave :1 FG600B3908600705
```

The command output shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this command to confirm that the cluster is operating normally. For example, if the command shows only one cluster unit then the other unit has left the cluster for some reason.

3. Check the cluster synchronization status to make sure the primary and backup units have the same configuration. Log into the primary unit CLI and enter this command:

```
diag sys ha cluster-csum
```

The CLI lists all members' checksums. If both cluster units have identical checksums you can be sure that their configurations are synchronized. If the checksums are different wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical contact Fortinet support to help troubleshoot the problem.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard do not display information for both cluster units the FortiGate units are not functioning as a cluster. See Setting up two new FortiGates as an FGCP cluster on page 1319 to troubleshoot the cluster.

To add basic configuration settings to the cluster

Use the following steps to add some basic settings to the cluster so that it can connect to the network.

1. Log into the primary unit CLI.
2. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <password_str>
end
```

3. Configure the port1 and port2 interfaces.

```
config system interface
   edit port1
      set ip 172.20.120.141/24
   next
   edit port2
      set ip 10.11.101.100/24
end
```

4. Add a default route.

```
config router static
   edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 172.20.120.2
      set device port1
end
```

Adding a new FortiGate to an operating cluster

This procedure describes how to add a new FortiGate unit to a functioning cluster. Adding a new unit to a cluster does not interrupt the operation of the cluster unless you have to change how the cluster is connected to the network to accommodate the new cluster unit.

You can use this procedure to add as many units as required to the cluster.

To add a new unit to a functioning cluster

1. Install the same firmware build on the new cluster unit as is running on the cluster.
2. Register and apply licenses to the new cluster unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS). FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. Configure the new cluster unit for HA operation with the same HA configuration as the other units in the cluster.
4. If the cluster is running in Transparent mode, change the operating mode of the new cluster unit to Transparent mode.
5. Power off the new cluster unit.
6. Connect the new cluster unit to the cluster.
7. For example, see How to set up FGCP clustering (recommended steps) on page 1313.
8. Power on the new cluster unit.

   When the unit starts it negotiates to join the cluster. After it joins the cluster, the cluster synchronizes the new unit configuration with the configuration of the primary unit.

You can add a new unit to a functioning cluster at any time. The new cluster unit must:

- Have the same hardware configuration as the cluster units. Including the same hard disk configuration and the same AMC cards installed in the same slots.
- Have the same firmware build as the cluster.
- Be set to the same operating mode (NAT or Transparent) as the cluster.
- Be operating in single VDOM mode.

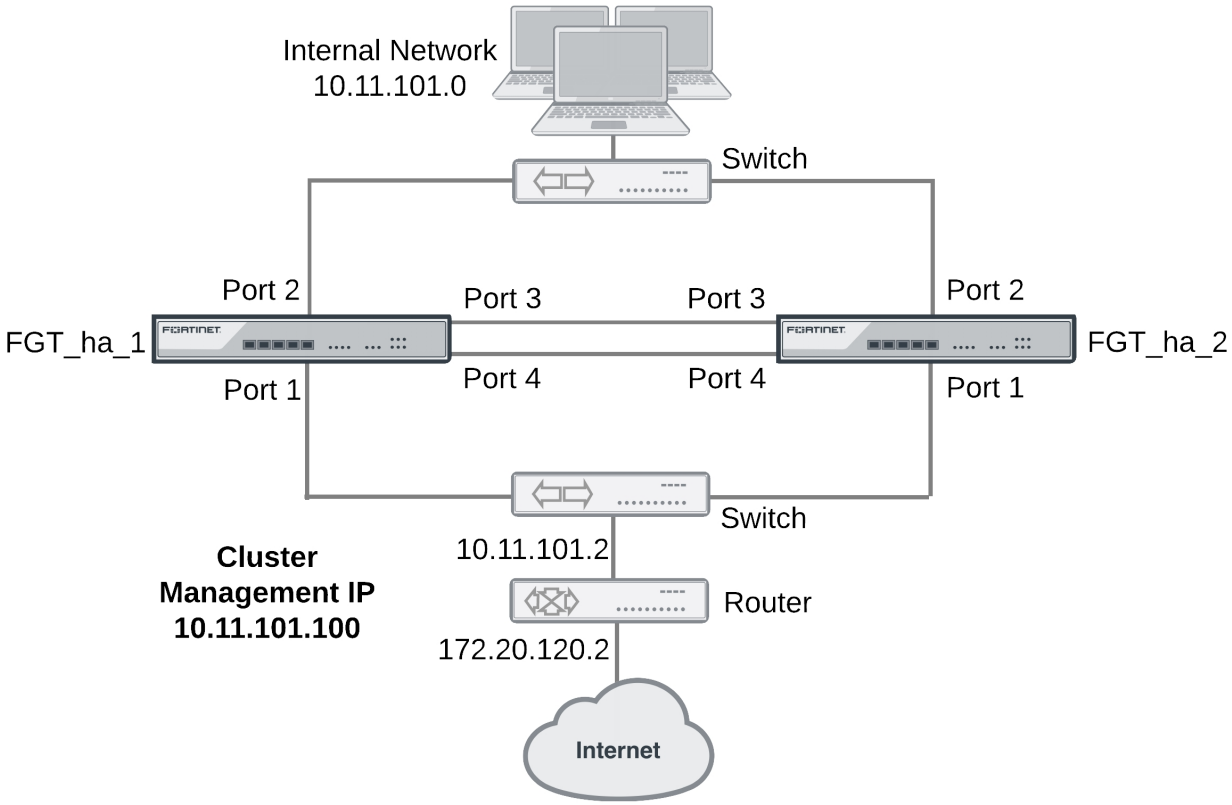
Active-active HA cluster in Transparent mode

This section describes a simple HA network topology that includes an HA cluster of two generic FortiGate units installed between an internal network and the Internet and running in Transparent mode.

Example Transparent mode HA network topology

The figure below shows a Transparent mode FortiGate HA cluster consisting of two FortiGate units (FGT_ha_1 and FGT_ha_2) installed between the Internet and internal network. The topology includes a router that performs NAT between the internal network and the Internet. The cluster management IP address is 10.11.101.100.

Transparent mode HA network topology



Port3 and port4 are used as the heartbeat interfaces. Because the cluster consists of two FortiGate units, you can make the connections between the heartbeat interfaces using crossover cables. You could also use switches and regular ethernet cables.

General configuration steps

This section includes web-based manager and CLI procedures. These procedures assume that the FortiGate units are running the same FortiOS firmware build and are set to the factory default configuration.

In this example, the configuration steps are identical to the NAT/Route mode configuration steps until the cluster is operating. When the cluster is operating, you can switch to Transparent mode and add basic configuration settings to cluster.

General configuration steps

1. Apply licenses to the FortiGate units to become the cluster.
2. Configure the FortiGate units for HA operation.
   - Optionally change each unit's host name.
   - Configure HA.
2. Connect the cluster to the network.
3. Confirm that the cluster units are operating as a cluster.

4. Switch the cluster to Transparent mode and add basic configuration settings to the cluster.
   - Switch to Transparent mode, add the management IP address and a default route.
   - Add a password for the admin administrative account.
   - View cluster status from the web-based manager or CLI.

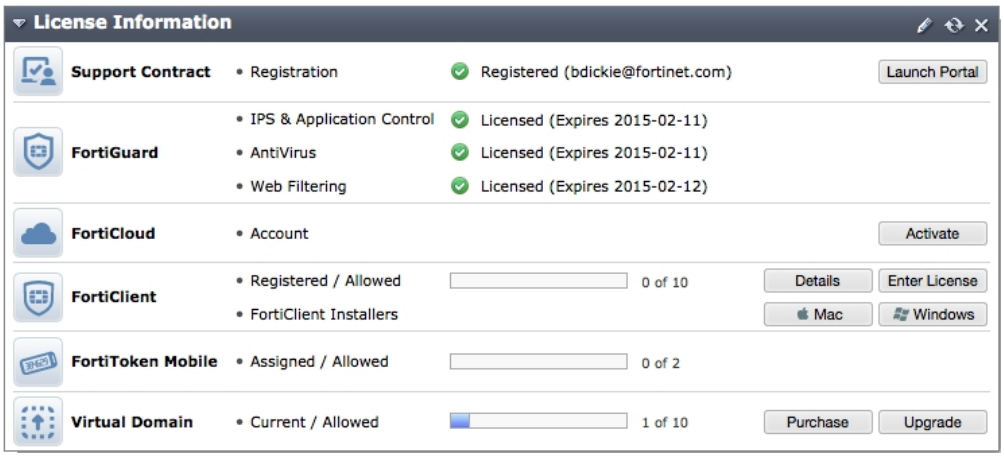
Configuring a Transparent mode active-active cluster of two FortiGate units - web-based manager

Use the following procedures to configure the FortiGate units for HA operation using the FortiGate web-based manager. These procedures assume you are starting with two FortiGate units with factory default settings.

Waiting until you have established the cluster to switch to Transparent mode means fewer configuration steps because you can switch the mode of the cluster in one step.

To configure the first FortiGate unit (host name FGT_ha_1)

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Select **OK**.
6. Go to **System > Config > HA** and change the following settings:

Mode	Active-Active
Group Name	example2.com
Password	HA_pass_2

This is the minimum recommended configuration for an active-active HA cluster. You can configure other HA options at this point, but if you wait until the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

7. Select **OK**.

   The FortiGate unit negotiates to establish an HA cluster. When you select **OK** you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

   - port1 interface virtual MAC: `00-09-0f-09-00-00`
   - port2 interface virtual MAC: `00-09-0f-09-00-01`
   - port3 interface virtual MAC: `00-09-0f-09-00-02`
   - port4 interface virtual MAC: `00-09-0f-09-00-03`

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

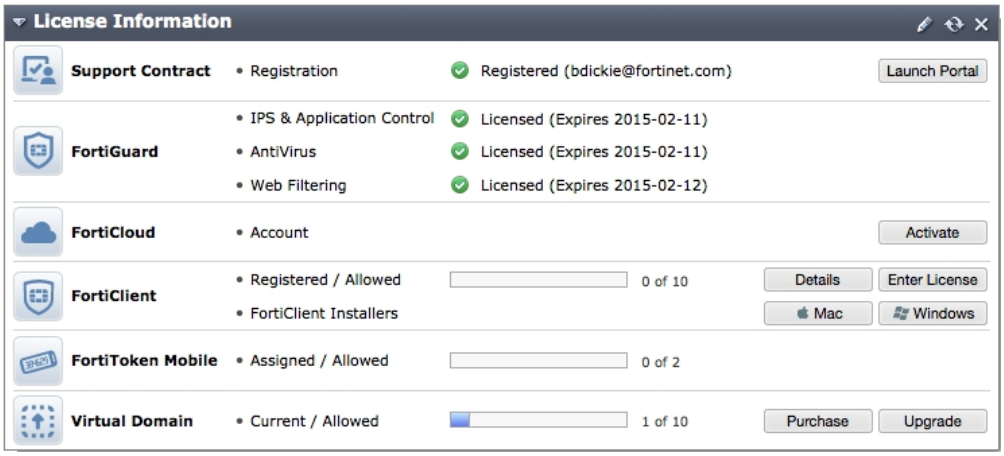
   To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`MAC`) and the port1 permanent MAC address (`Permanent_HWaddr`):

   ```
   get hardware nic port1
   .
   .
   .
   Current_HAaddr    00:09:0f:09:00:00
   Permanent_HWaddr  02:09:0f:78:18:c9
   .
   .
   .
   ```

10. Power off the first FortiGate unit.

To configure the second FortiGate unit (host name FGT_ha_2)

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
3. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_2

4. Select **OK**.
5. Go to **System > Config > HA** and change the following settings:

Mode	Active-Active
Group Name	example2.com
Password	HA_pass_2

6. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces.

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.
7. Power off the second FortiGate unit.

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
3. Connect the port3 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation

occurs with no user intervention and normally takes less than a minute.

When negotiation is complete the cluster is ready to be configured for your network.

To switch the cluster to Transparent mode

Switching from NAT/Route to Transparent mode involves adding the Transparent mode management IP address and default route.

This is the minimum recommended configuration for an active-active HA cluster. You can configure other HA options at this point, but if you wait until the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

1. Start a web browser and browse to the address `https://192.168.1.99` (remember to include the “s” in `https://`).
   The FortiGate Login is displayed.
2. Type admin in the Name field and select Login.
3. Under System Information, beside **Operation Mode** select **Change**.
4. Set Operation Mode to Transparent.
5. Configure basic Transparent mode settings.

Operation Mode	Transparent
Management IP/Mask	10.11.101.100/24
Default Gateway	10.11.101.2

6. Select **Apply**.
   The cluster switches to operating in Transparent mode. The virtual MAC addresses assigned to the cluster interfaces do not change.

To view cluster status

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster.

Once the cluster is operating, because configuration changes are synchronized to all cluster units, configuring the cluster is the same as configuring an individual FortiGate unit. You could have performed the following configuration steps separately on each FortiGate unit before you connected them to form a cluster.

1. Start Internet Explorer and browse to the address https://10.11.101.100 (remember to include the “s” in https://).
   The FortiGate Login is displayed.
2. Type admin in the Name field and select Login.
   The FortiGate dashboard is displayed.

The System Information dashboard widget shows the **Cluster Name** (example2.com) and the host names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.

3. Go to **System > Config > HA** to view the cluster members list.
   The list shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this list to confirm that the cluster is operating normally. For example, if the list shows only one cluster unit then the other unit has left the cluster for some reason.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard do not display information for both cluster units, the FortiGate units are not functioning as a cluster. See Active-active HA cluster in Transparent mode on page 1331 to troubleshoot the cluster.

To add basic configuration settings to the cluster

Use the following steps to configure the cluster. Note that the following are example configuration steps only and do not represent all of the steps required to configure the cluster for a given network.

1. Log into the cluster web-based manager.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.
5. Select **OK**.

You added a default gateway when you switched to Transparent mode so you don't need to add a default route as part of the basic configuration of the cluster at this point.

Configuring a Transparent mode active-active cluster of two FortiGate units - CLI

Use the following procedures to configure the FortiGate units for Transparent mode HA operation using the FortiGate CLI.

To configure each FortiGate unit for HA operation

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal, enter a name for the connection, and select **OK**.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select **OK**.
5. Select the following port settings and select **OK**.

Bits per second	9600
Data bits	8

Parity	None
Stop bits	1
Flow control	None

6. Press **Enter** to connect to the FortiGate CLI.
   The FortiGate unit CLI login prompt appears.If the prompt does not appear, press Enter. If it still does not appear, power off your FortiGate unit and power it back on. If you are connected, at this stage you will see startup messages that will confirm you are connected. The login prompt will appear after the startup has completed.
7. Type `admin` and press **Enter** twice.
8. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
9. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
10. Change the host name for this FortiGate unit. For example:
```
config system global
   set hostname FGT_ha_1
end
```
11. Configure HA settings.
```
config system ha
   set mode a-a
   set group-name example2.com
   set password HA_pass_2
end
```

This is the minimum recommended configuration for an active-active HA cluster. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose network connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port2 interface virtual MAC: `00-09-0f-09-00-01`
- port3 interface virtual MAC: `00-09-0f-09-00-02`
- port4 interface virtual MAC: `00-09-0f-09-00-03`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate

unit interface. For example, use the following command to view the port1 interface virtual MAC address (`MAC`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
Current_HAaddr    00:09:0f:09:00:00
Permanent_HWaddr  02:09:0f:78:18:c9
.
.
.
```

10. Display the HA configuration (optional).

```
get system ha
   group-id : 0
   group-name : example2.com
   mode : a-a
   password : *
   hbdev : "port3" 50 "port4" 50
   session-sync-dev    :
   route-ttl : 10
   route-wait : 0
   route-hold : 10
   sync-config : enable
   encryption : disable
   authentication : disable
   hb-interval : 2
   hb-lost-threshold : 20
   helo-holddown : 20
   arps : 5
   arps-interval : 8
   session-pickup : disable
   update-all-session-timer: disable
   session-sync-daemon-number: 1
   link-failed-signal : disable
   uninterruptible-upgrade: enable
   ha-mgmt-status : disable
   ha-eth-type : 8890
   hc-eth-type : 8891
   l2ep-eth-type : 8893
   ha-uptime-diff-margin: 300
   vcluster2 : disable
   vcluster-id : 1
   override : disable
   priority : 128
   slave-switch-standby: disable
   minimum-worker-threshold: 1
   monitor :
   pingserver-monitor-interface:
   pingserver-failover-threshold: 0
   pingserver-slave-force-reset: enable
   pingserver-flip-timeout: 60
   vdom : "root"
```

11. Power off the FortiGate unit.

To configure the second FortiGate unit (host name FGT_ha_2)

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal, enter a name for the connection, and select **OK**.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select **OK**.
5. Select the following port settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press **Enter** to connect to the FortiGate CLI.

   The FortiGate unit CLI login prompt appears.If the prompt does not appear, press Enter. If it still does not appear, power off your FortiGate unit and power it back on. If you are connected, at this stage you will see startup messages that will confirm you are connected. The login prompt will appear after the startup has completed.
7. Type `admin` and press **Enter** twice.
8. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
9. Change the host name for this FortiGate unit.

```
config system global
   set hostname FGT_ha_2
end
```

10. Configure HA settings.

```
config system ha
   set mode a-a
   set group-name example2.com
   set password HA_pass_2
end
```

    The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose network connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces.

    To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.
11. Display the HA configuration (optional).

```
get system ha
   group-id : 0
   group-name : example2.com
   mode : a-a
```

```
password : *
hbdev : "port3" 50 "port4" 50
session-sync-dev    :
route-ttl : 10
route-wait : 0
route-hold : 10
sync-config : enable
encryption : disable
authentication : disable
hb-interval : 2
hb-lost-threshold : 20
helo-holddown : 20
arps : 5
arps-interval : 8
session-pickup : disable
update-all-session-timer: disable
session-sync-daemon-number: 1
link-failed-signal : disable
uninterruptible-upgrade: enable
ha-mgmt-status : disable
ha-eth-type : 8890
hc-eth-type : 8891
l2ep-eth-type : 8893
ha-uptime-diff-margin: 300
vcluster2 : disable
vcluster-id : 1
override : disable
priority : 128
schedule : round-robin
monitor :
pingserver-monitor-interface:
pingserver-failover-threshold: 0
pingserver-slave-force-reset: enable
pingserver-flip-timeout: 60
vdom : "root"
schedule : round-robin
```

12. Power off the FortiGate unit.

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
3. Connect the port3 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.

   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete the cluster is ready to be configured for your network.

To connect to the cluster CLI and switch the cluster to Transparent mode

1. Determine which cluster unit is the primary unit.
   - Use the null-modem cable and serial connection to re-connect to the CLI of one of the cluster units.
   - Enter the command `get system status`.
   - If the command output includes `Current HA mode: a-a, master`, the cluster units are operating as a cluster and you have connected to the primary unit. Continue with Step 2.
   - If the command output includes `Current HA mode: a-a, backup`, you have connected to a subordinate unit. Connect to the other cluster unit, which should be the primary unit and continue with Step 2.

If the command output includes `Current HA mode: standalone`, the cluster unit is not operating in HA mode.

2. Change to transparent mode.

```
config system settings
   set opmode transparent
   set manageip 192.168.20.3/24
   set gateway 192.168.20.1
end
```

   The cluster switches to Transparent Mode, and your administration session is disconnected.

   You can now connect to the cluster CLI using SSH to connect to the cluster internal interface using the management IP address (192.168.20.3).

To view cluster status

Use the following steps to view cluster status from the CLI.

1. Determine which cluster unit is the primary unit.
   - Use the null-modem cable and serial connection to re-connect to the CLI of one of the cluster units.
   - Enter the command `get system status`.
   - If the command output includes `Current HA mode: a-a, master`, the cluster units are operating as a cluster and you have connected to the primary unit. Continue with Step "Active-active HA cluster in Transparent mode" on page 1331.
   - If the command output includes `Current HA mode: a-a, backup`, you have connected to a subordinate unit. Connect the null-modem cable to the other cluster unit, which should be the primary unit and continue with Step 2.

If the command output includes `Current HA mode: standalone`, the cluster unit is not operating in HA mode and you should review your HA configuration.

2. Enter the following command to confirm the HA configuration of the cluster:

```
get system ha status
   Model: XXXX
   Mode: a-a
   Group: 0
   Debug: 0
   ses_pickup: disable
```

```
Master:128 FGT_ha_2 FG600B3908600825 0
Slave :128 FGT_ha_1 FG600B3908600705 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG600B3908600825
Slave :1 FG600B3908600705
```

The command output shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this command to confirm that the cluster is operating normally. For example, if the command shows only one cluster unit then the other unit has left the cluster for some reason.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard do not display information for both cluster units the FortiGate units are not functioning as a cluster. See Active-active HA cluster in Transparent mode on page 1331to troubleshoot the cluster.

To add a password for the admin administrative account

1. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <psswrd>
end
```

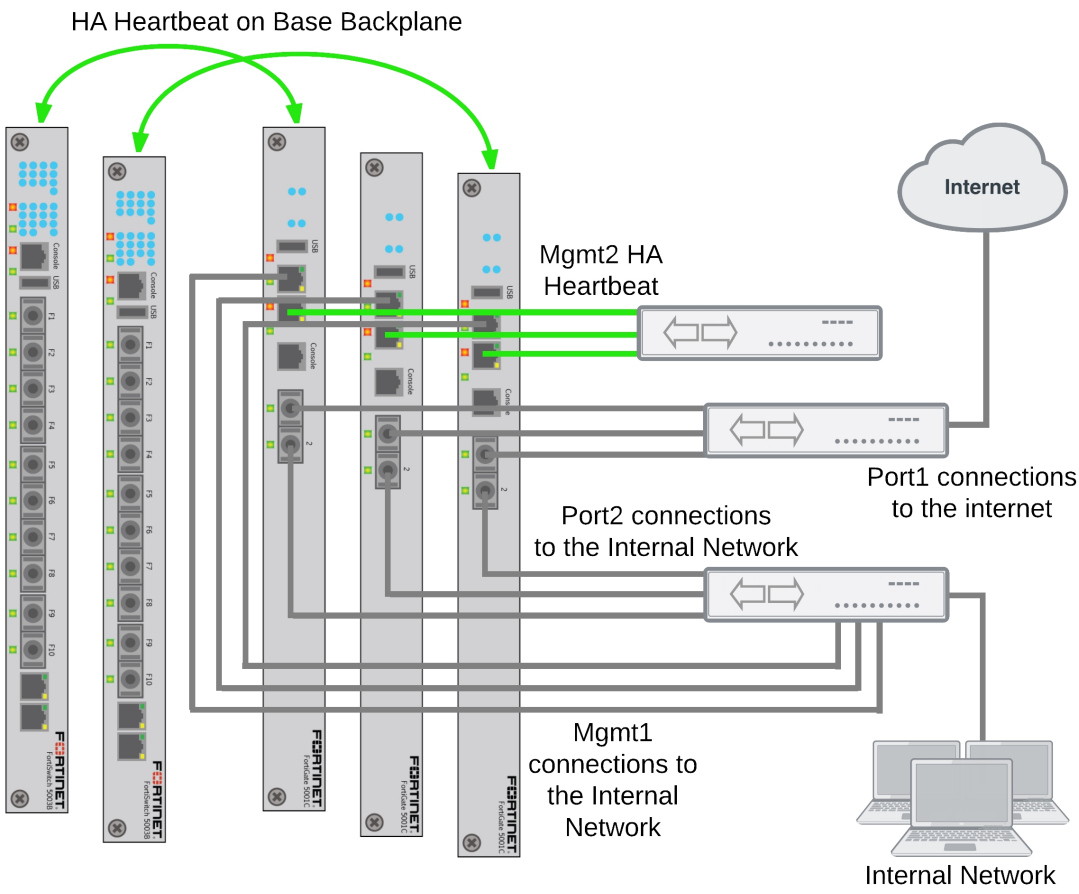
FortiGate-5000 active-active HA cluster with FortiClient licenses

This section describes how to configure an HA cluster of three FortiGate-5001C units that connect an internal network to the Internet. The FortiGate-5001C units each have a FortiClient license installed on them to support FortiClient profiles.

Normally it is recommended that you add FortiClient licenses to the FortiGate units before setting up the cluster. This example; however, describes how to apply FortiClient licenses to the FortiGate units in an operating cluster.

Example network topology

The following diagram shows an HA cluster consisting of three FortiGate-5001C cluster units (host names slot-3, slot-4, and slot-5) installed in a FortiGate-5000 series chassis with two FortiSwitch-5003B units for heartbeat communication between the cluster units. The cluster applies security features including FortiClient profiles to data traffic passing through it.



The cluster is managed from the internal network using the FortiGate-5001C mgmt1 interfaces configured as HA reserved management interfaces. Using these reserved management interfaces the overall cluster can be managed and cluster units can be managed individually. Individual management access to each cluster unit makes some operations, such as installing FortiClient licenses, easier and also allows you to view status of each cluster unit.

The reserved management interface of each cluster unit has a different IP address and retains its own MAC address. The cluster does not change the reserved management interface MAC address.

Example network topology

By default base1 and base2 are used for heartbeat communication between the FortiGate units. To use the base1 and base2 interfaces for the HA heartbeat, the example describes how to display the backplane interfaces on the web-based manager before turning on HA.

This example also includes using the mgmt2 interface for heartbeat communication for additional heartbeat redundancy.

To connect the cluster

1. Connect the FortiGate-5001C port1 interfaces to a switch and connect that switch to the Internet.
2. Connect the FortiGate-5001C port2 interfaces to a switch and connect that switch to the internal network.

3. Connect the FortiGate-5001C mgmt1 interfaces to a switch that connects to the engineering network.
4. Connect the FortiGate-5001C mgmt2 interfaces to a switch for heartbeat communication between them.

Configuring the FortiGate-5000 active-active cluster - web-based manager

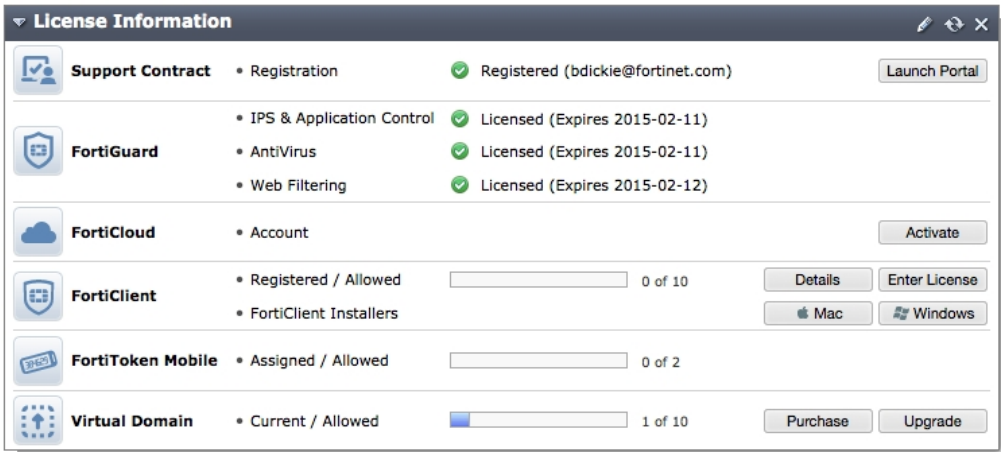
These procedures assume you are starting with three FortiGate-5001C boards and two FortiSwitch-5003B boards installed in a compatible FortiGate-5000 series chassis. The FortiSwitch-5003B boards are in chassis slots 1 and 2 and the FortiGate-5001C boards are in chassis slots 3, 4, and 5 and the chassis is powered on. All devices are in their factory default configuration. No configuration changes to the FortiSwitch-5003B boards are required.

To configure the FortiGate-5001C units

1. From the internal network, log into the web-based manager of the FortiGate-5001C unit in chassis slot 3 by connecting to the mgmt1 interface.

By default the mgmt1 interface of each FortiGate-5001C unit has the same IP address. To log into each FortiGate-5001C unit separately you could either disconnect the mgmt1 interfaces of the units that you don't want to log into or change the mgmt1 interface IP addresses for each unit by connecting to each unit's CLI from their console port.

2. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS). In this example you will leave **FortiClient** licensing until after you have formed the cluster.



3. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
4. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
5. Enter a new Host Name for this FortiGate unit, for example:

New Name	5001C-Slot-3

6. Connect to the CLI and enter the following command to display backplane interfaces on the web-based manager:

```
config system global
   set show-backplane-intf enable
end
```

7. Set the Administrative Status of the base1 and base 2 interfaces to **Up**.
   You can do this from the web-based manager by going to **System > Network > Interface**, editing each interface and setting **Administrative Status** to **Up**.

   You can also do this from the CLI using the following command:

```
config system interface
   edit base1
      set status up
   next
   edit base2
      set status up
   end
```

8. Go to **System > Network > Interface** and configure the IP address of the mgmt1 interface.
   Because mgmt1 will become the reserved management interface for the cluster unit each FortiGate-5001C should have a different mgmt1 interface IP address. Give the mgmt1 interface an address that is valid for the internal network. Once HA with the reserved Management interface is enabled the IP address of the mgmt1 interface can be on the same subnet as the port2 interface (which will also be connected to the Internal network).

   After the FortiGate unit is operating in HA mode the mgmt1 interface will retain its original MAC address instead of being assigned a virtual MAC address.

9. Go to **System > Config > HA** and change the following settings:
   Set the **Mode** to **Active-Active**.

   Select **Reserve Management Port for Cluster Member** and select **mgmt1**.

   Set the group name and password:

Group Name	example3.com
Password	HA_pass_3

   Set the Heartbeat interface configuration to use base1, base2 and mgmt2 for heartbeat communication. Set the priority of each heartbeat interface to 50:

	Heartbeat Interface	
	Enable	**Priority**
base1	Select	50
base2	Select	50
mgmt2	Select	50

10. Select **OK**.
    The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate-5001C interfaces change to the following virtual MAC addresses:

- base1 interface virtual MAC: `00-09-0f-09-00-00`
- base2 interface virtual MAC: `00-09-0f-09-00-01`
- fabric1 interface virtual MAC: `00-09-0f-09-00-02`
- fabric2 interface virtual MAC: `00-09-0f-09-00-03`
- fabric3 interface virtual MAC: `00-09-0f-09-00-04`
- fabric4 interface virtual MAC: `00-09-0f-09-00-05`
- fabric5 interface virtual MAC: `00-09-0f-09-00-06`
- mgmt1 keeps its original MAC address
- mgmt2 interface virtual MAC: `00-09-0f-09-00-08`
- port1 interface virtual MAC: `00-09-0f-09-00-09`
- port2 interface virtual MAC: `00-09-0f-09-00-0a`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic base1
.
.
.
Current_HWaddr 00:09:0f:09:00:00
Permanent_HWaddr 00:09:0f:71:0a:dc
.
.
.
```

9. Repeat these steps for the FortiGate-5001C units in chassis slots 4 and 5, with the following differences.
   Set the mgmt1 interface IP address of each FortiGate-5001C unit to a different IP address.

   Set the FortiGate-5001C unit in chassis slot 4 host name to:

New Name	5001C-Slot-4

   Set the FortiGate-5001C unit in chassis slot 5 host name to:

New Name	5001C-Slot-5

   As you configure each FortiGate unit, they will negotiate and join the cluster.

To view cluster status

As you add units to the cluster you can log into the web-based manager of one of the cluster units to view the status of the cluster. The status displays will show each unit as it is added to the cluster.

1. Log into the primary unit or any cluster unit and view the system dashboard.
   The System Information dashboard widget shows the **Cluster Name** (example3.com) and the host

names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.

2. Go to **System > Config > HA** to view the cluster members list.
   The list shows three cluster units, their host names, their roles in the cluster, and their priorities. You can check this list at any time to confirm that the cluster is operating normally.

   If the cluster members list and the dashboard do not display all of the cluster units, they are not functioning as a cluster.

To troubleshoot the cluster

See FortiGate-5000 active-active HA cluster with FortiClient licenses on page 1343.

To manage each cluster unit

Because you have configured a reserved management interface, you can manage each cluster unit separately by connecting to the IP address you configured for each unit's mgmt1 interface. You can view the status of each cluster unit and make changes to each unit's configuration. For example, as described below, each cluster unit must have its own FortiClient license. You can use the reserved management IP addresses to connect to each cluster unit to install the FortiClient license for that unit.

Usually you would make configuration changes by connecting to the primary unit and changing its configuration. The cluster then synchronizes the configuration changes to all cluster units. If you connect to individual cluster units and change their configuration, those configuration changes are also synchronized to each cluster unit. The exception to this is configuration objects that are not synchronized, such as the host name, FortiClient license and so on.

You can also manage each cluster unit by logging into the primary unit CLI and using the following command to connect to other cluster units:

```
execute ha manage <cluster-index>
```

To add basic configuration settings to the cluster

Use the following steps to configure the cluster.

1. Log into the cluster web-based manager.
   You can log into the primary unit or any one of the cluster units using the appropriate mgmt1 IP address.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.
5. Select **OK**.
6. Go to **System > Network > Interface** and edit the **port1** interface. Set this interface IP address to the address required to connect to the interface to the Internet.
7. Edit the port2 interface and set its IP to an IP address for the internal network.

To add a FortiClient license to each cluster unit

Normally you would add FortiClient licenses to the FortiGate units before forming the cluster. However, you can can use the following steps to add FortiClient licenses to an operating cluster.

Contact your reseller to purchase FortiClient licenses for your cluster units. Each cluster unit must have its own FortiClient license.

When you receive the license keys you can log into https://support.fortinet.com and add a FortiClient license key to each licensed FortiGate unit. Then, as long as the cluster can connect to the Internet the license keys are downloaded from the FortiGuard network to all of the FortiGate units in the cluster.

You can also use the following steps to manually add the license keys to your cluster units from the web-based manager. Your cluster must be connected to the Internet.

1. Log into the -web-based manager of each cluster unit using its reserved management interface IP address.
2. Go to the **License Information** dashboard widget and beside FortiClient select **Enter License**.
3. Enter the license key and select **OK**.
4. Confirm that the license has been installed and the correct number of FortiClients are licensed.
5. Repeat for all of the cluster units.

You can also use the following command to add the license key from the CLI:

```
execute FortiClient-NAC update-registration-license <license-number>
```

You can connect to the CLIs of each cluster unit using their reserved management IP address.

You can also log into the primary unit CLI and use the `execute ha manage` command to connect to each cluster unit CLI.

Configuring the FortiGate-5000 active-active cluster - CLI

These procedures assume you are starting with three FortiGate-5001C boards and two FortiSwitch-5003B boards installed in a compatible FortiGate-5000 series chassis. The FortiSwitch-5003B boards are in chassis slots 1 and 2 and the FortiGate-5001C boards are in chassis slots 3, 4, and 5 and the chassis is powered on. All devices are in their factory default configuration. No configuration changes to the FortiSwitch-5003B boards are required.

To configure the FortiGate-5005FA2 units

1. From the internal network, log into the CLI of the FortiGate-5001C unit in chassis slot 3 by connecting to the mgmt1 interface.

By default the mgmt1 interface of each FortiGate-5001C unit has the same IP address. To log into each FortiGate-5001C unit separately you could either disconnect the mgmt1 interfaces of the units that you don't want to log into or change the mgmt1 interface IP addresses for each unit by connecting to each unit's CLI from their console port.

   You can also use a console connection.

2. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS). In this example you will leave **FortiClient** licensing until after you have formed the cluster.
3. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
4. Change the host name for this FortiGate unit. For example:

```
config system global
  set hostname 5001C-Slot-3
end
```

5. Enter the following command to display backplane interfaces on the web-based manager:

```
config system global
   set show-backplane-intf enable
end
```

6. Set the Administrative Status of the base1 and base 2 interfaces to **Up**.

```
config system interface
   edit base1
      set status up
   next
   edit base2
      set status up
   end
```

7. Add an IP address to the mgmt1 interface.

```
config system interface
   edit mgmt1
      set ip 172.20.120.110/24
      set allowaccess http https ssl ping
   end
```

   Because mgmt1 will become the reserved management interface for the cluster unit each FortiGate-5001C should have a different mgmt1 interface IP address. Give the mgmt1 interface an address that is valid for the internal network. Once HA with the reserved Management interface is enabled the IP address of the mgmt1 interface can be on the same subnet as the port2 interface (which will also be connected to the Internal network).

8. Configure HA settings.

```
config system ha
   set mode a-a
   set ha-mgmt-status enable
   set ha-mgmt-interface mgmt1
   set group-name example3.com
   set password HA_pass_3
   set hbdev base1 50 base2 50 mgmt2 50
end
```

   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate-5001C interfaces change to the following virtual MAC addresses:

   - base1 interface virtual MAC: `00-09-0f-09-00-00`
   - base2 interface virtual MAC: `00-09-0f-09-00-01`
   - fabric1 interface virtual MAC: `00-09-0f-09-00-02`
   - fabric2 interface virtual MAC: `00-09-0f-09-00-03`
   - fabric3 interface virtual MAC: `00-09-0f-09-00-04`
   - fabric4 interface virtual MAC: `00-09-0f-09-00-05`
   - fabric5 interface virtual MAC: `00-09-0f-09-00-06`
   - mgmt1 keeps its original MAC address
   - mgmt2 interface virtual MAC: `00-09-0f-09-00-08`

- port1 interface virtual MAC: `00-09-0f-09-00-09`
- port2 interface virtual MAC: `00-09-0f-09-00-0a`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic base1
.
.
.
Current_HWaddr 00:09:0f:09:00:00
Permanent_HWaddr 00:09:0f:71:0a:dc
.
.
.
```

7. Repeat these steps for the FortiGate-5001C units in chassis slots 4 and 5, with the following differences.

   Set the mgmt1 interface IP address of each FortiGate-5001C unit to a different IP address.

   Set the FortiGate-5001C unit in chassis slot 4 host name to:

   ```
   config system global
      set hostname 5001C-Slot-4
   end
   ```

   Set the FortiGate-5001C unit in chassis slot 5 host name to:

   ```
   config system global
      set hostname 5001C-Slot-5
   end
   ```

   As you configure each FortiGate unit, they will negotiate and join the cluster.

To view cluster status

As you add units to the cluster you can log into the CLI of one of the cluster units using its reserved management interface to view the status of the cluster. The status will show each unit as it is added to the cluster.

For example, the following command output shows the status of the cluster when all three cluster units have been added:

```
get system ha status
Model: FortiGate-5001C
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
Master:128 slot-5      FG-5KC3E13800084 0
Slave :128 slot-4 FG-5KC3E13800051 1
Slave :128 slot-3 FG-5KC3E13800046 2
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG-5KC3E13800084
```

```
Slave :1 FG-5KC3E13800051
Slave :2 FG-5KC3E13800046
```

You can use this command to confirm that the cluster is operating normally. For example, if the command shows only two cluster units then one unit has left the cluster for some reason.

To troubleshoot the cluster

See FortiGate-5000 active-active HA cluster with FortiClient licenses on page 1343.

To manage each cluster unit

Because you have configured a reserved management interface, you can manage each cluster unit separately by connecting to the IP address you configured for each unit's mgmt1 interface. You can view the status of each cluster unit and make changes to each unit's configuration. For example, as described below, each cluster unit must have its own FortiClient license. You can use the reserved management IP addresses to connect to each cluster unit to install the FortiClient license for that unit.

Usually you would make configuration changes by connecting to the primary unit and changing its configuration. The cluster then synchronizes the configuration changes to all cluster units. If you connect to individual cluster units and change their configuration, those configuration changes are also synchronized to each cluster unit. The exception to this is configuration objects that are not synchronized, such as the host name, FortiClient license and so on.

You can also manage each cluster unit by logging into the primary unit CLI and using the following command to connect to other cluster units:

```
execute ha manage <cluster-index>
```

To add a password for the admin administrative account

1. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <psswrd>
end
```

To add basic configuration settings to the cluster

Use the following steps to configure the cluster.

1. Log into the cluster CLI.

   You can log into the primary unit or any one of the cluster units using the appropriate mgmt1 IP address.

2. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <psswrd>
end
```

3. Set the port1 interface IP address to the address required to connect to the interface to the Internet.

```
config system interface
   edit port1
      set ip 10.10.10.10/24
   end
```

4. Set the port2 interface IP address to the address required to connect to the interface to the internal network.

```
config system interface
  edit port2
    set ip 172.20.120.12/24
  end
```

To add a FortiClient license to each cluster unit

Normally you would add FortiClient licenses to the FortiGate units before forming the cluster. However, you can can use the following steps to add FortiClient licenses to an operating cluster.

Contact your reseller to purchase FortiClient licenses for your cluster units. Each cluster unit must have its own FortiClient license.

When you receive the license keys you can log into https://support.fortinet.com and add a FortiClient license key to each licensed FortiGate unit. Then, as long as the cluster can connect to the Internet the license keys are downloaded from the FortiGuard network to all of the FortiGate units in the cluster.

You can also use the following steps to manually add the license keys to your cluster units from the CLI. Your cluster must be connected to the Internet.

1. Log into the CLI of each cluster unit using its reserved management interface IP address.
2. Enter the following command to the unit's serial number:

```
get system status
```

3. Enter the following command to add the license key for that serial number:

```
execute FortiClient-NAC update-registration-license <license-key>
```

4. Confirm that the license has been installed and the correct number of FortiClients are licensed.

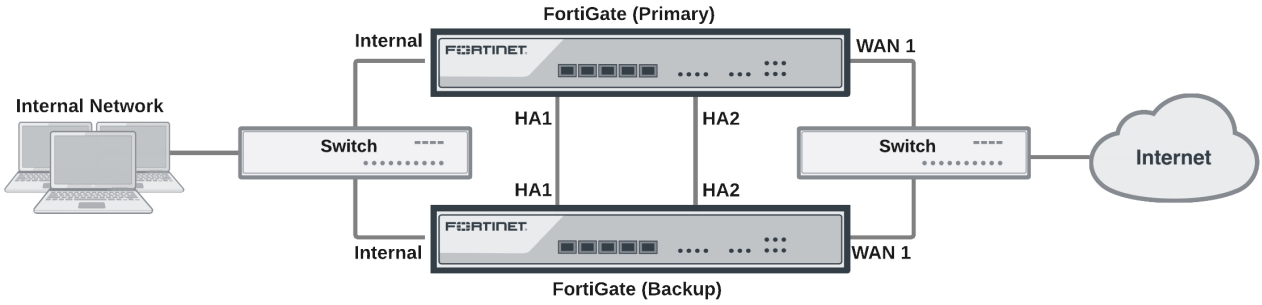
```
execute forticlient info
Maximum FortiClient connections: unlimited.
Licensed connections: 114
     NAC: 114
WANOPT: 0
Test: 0
Other connections:
     IPsec: 0
     SSLVPN: 0
```

5. Repeat for all of the cluster units.

You can also log into the primary unit CLI and use the `execute ha manage` command to connect to each cluster unit CLI.

Converting a standalone FortiGate unit to a cluster

In this recipe, a backup FortiGate unit will be installed and connected to a FortiGate unit that has previously been installed to provide redundancy if the primary FortiGate unit fails.

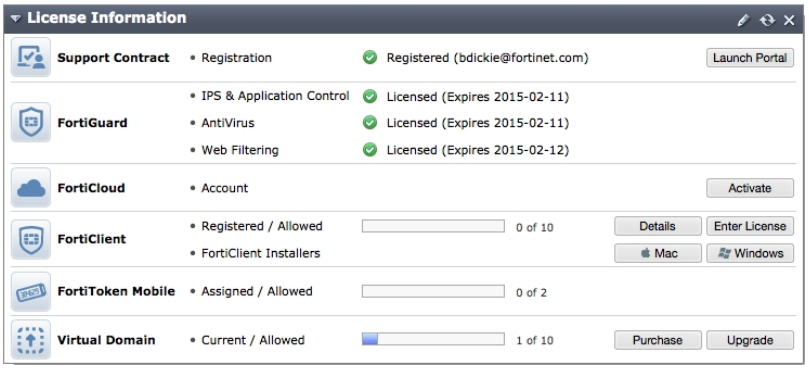


A video of this recipe is available here.

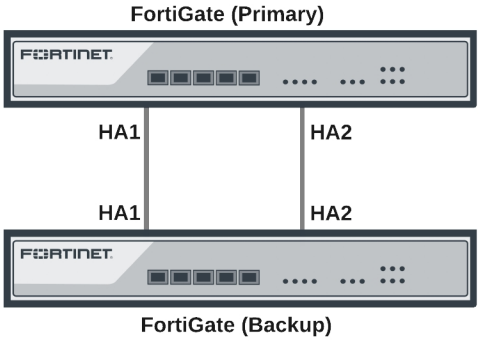
1. Adding the backup FortiGate unit and configuring HA

If the FortiGates in the cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

If you have not already done so, register the primary FortiGate and apply licenses to it before setting up the cluster. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate. FortiToken licenses can be added at any time because they are synchronized to all cluster members.

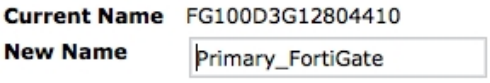


Connect your network as shown in the initial diagram, with Ethernet cables connecting the **HA** heartbeat interfaces of the two FortiGate units. If your FortiGate unit does not have dedicated HA heartbeat interfaces, you can use different interfaces, provided they are not used for any other function.



A switch must be used between the FortiGates and Internet, and another is required between the FortiGates and the internal network, as shown in the network diagram for this recipe.

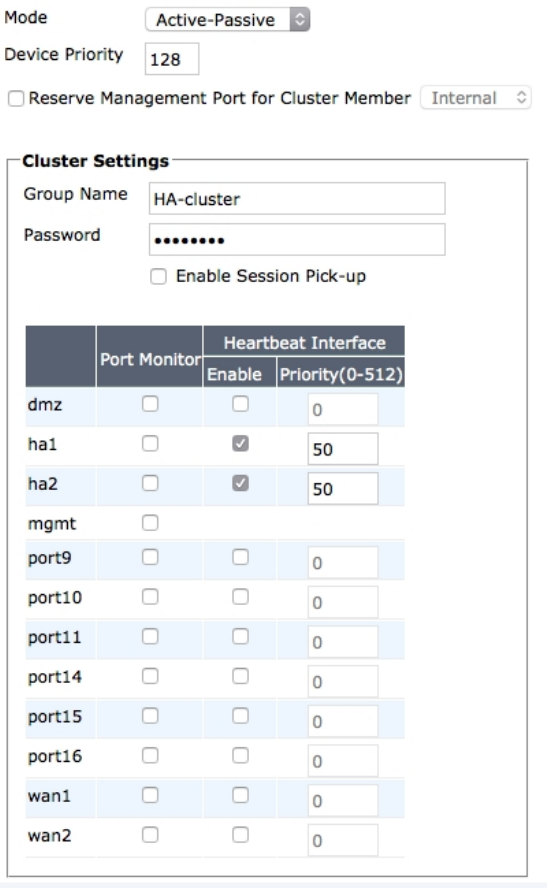
Connect to the primary FortiGate and go to **System > Dashboard > Status** and locate the **System Information** widget.



Change the unit's **Host Name** to identify it as the primary FortiGate.

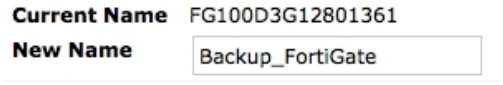
In the **System Information** widget, configure **HA Status**. Set the **Mode** to **Active-Passive** and set a **Group Name** and **Password**.

Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.



Connect to the backup FortiGate and go to **System > Dashboard > Status**.

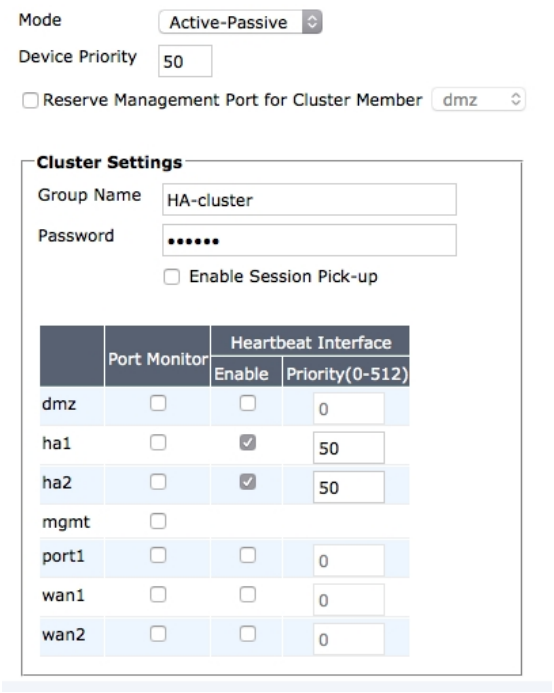
Change the unit's **Host Name** to identify it as the backup FortiGate.



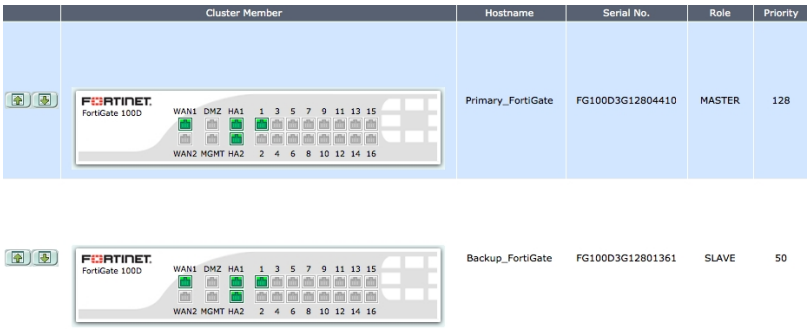
Configure **HA Status** and set the **Mode** to **Active-Passive**.

Set the **Device Priority** to be lower than the primary FortiGate. Ensure that the **Group Name** and **Password** match those on the primary FortiGate.

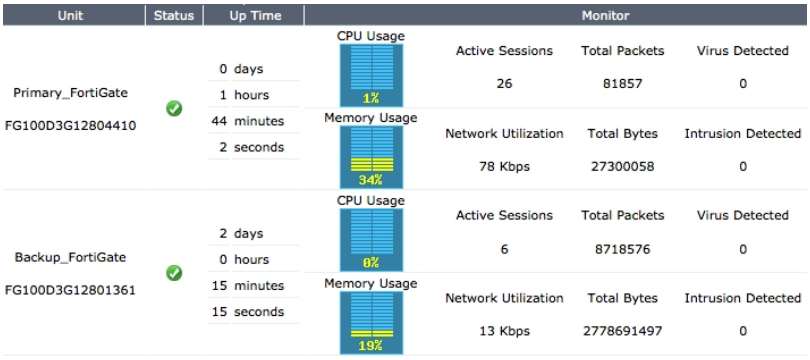
Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.



Connect to the primary FortiGate and go to **System > Config > HA** to view the cluster information.



Select **View HA Statistics** for more information on how the cluster is operating and processing traffic.



2. Results

Normally, traffic should now be flowing through the primary FortiGate. However, if the primary FortiGate is unavailable, traffic should failover and the backup FortiGate will be used. Failover will also cause the primary and backup FortiGates to reverse roles, even when both FortiGates are available again.

To test this, ping the IP address 8.8.8.8 using a PC on the internal network. After a moment, power off the primary FortiGate. You will see a momentary pause in the Ping results, until traffic diverts to the backup FortiGate, allowing the Ping traffic to continue.

```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

Replacing a failed cluster unit

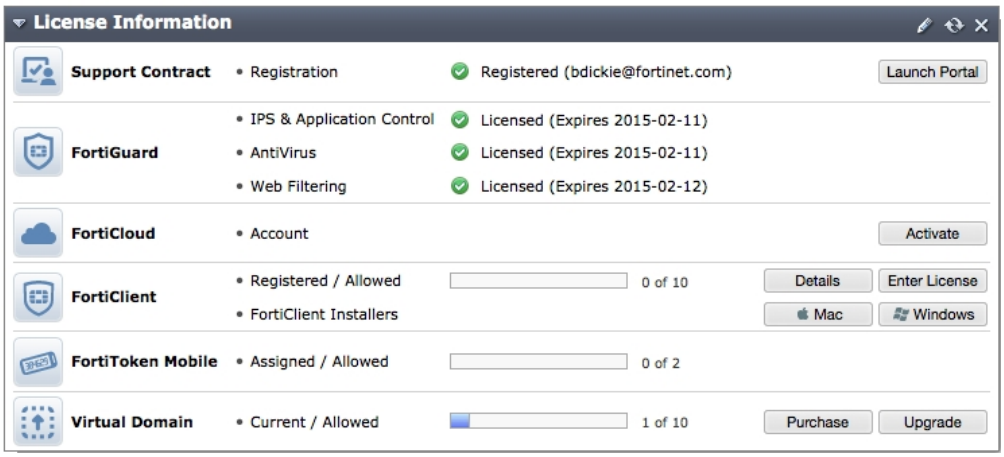
This procedure describes how to remove a failed cluster unit from a cluster and add a new one to replace it. You can also use this procedure to remove a failed unit from a cluster, repair it and add it back to the cluster. Replacing a failed does not interrupt the operation of the cluster unless you have to change how the cluster is connected to the network to accommodate the replacement unit.

You can use this procedure to replace more than one cluster unit.

To replace a failed cluster unit

1. Disconnect the failed unit from the cluster and the network.
   If you maintain other connections between the network and the still functioning cluster unit or units and between remaining cluster units network traffic will continue to be processed.
2. Repair the failed cluster unit, or obtain a replacement unit with the exact same hardware configuration as the failed cluster unit.
3. Install the same firmware build on the repaired or replacement unit as is running on the cluster.

4. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



5. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
6. Configure the repaired or replacement unit for HA operation with the same HA configuration as the cluster.
7. If the cluster is running in Transparent mode, change the operating mode of the repaired or replacement unit to Transparent mode.
8. Connect the repaired or replacement cluster unit to the cluster.
   For an example see: How to set up FGCP clustering (recommended steps) on page 1313.
9. Power on the repaired or replacement cluster unit.
   When the unit starts it negotiates to join the cluster. After it joins the cluster, the cluster synchronizes the repaired or replacement unit configuration with the configuration of the primary unit.

You can add a repaired or replacement unit to a functioning cluster at any time. The repaired or replacement cluster unit must:

- Have the same hardware configuration as the cluster units. Including the same hard disk configuration and the same AMC cards installed in the same slots.
- Have the same firmware build as the cluster.
- Be set to the same operating mode (NAT or Transparent) as the cluster.
- Be operating in single VDOM mode.

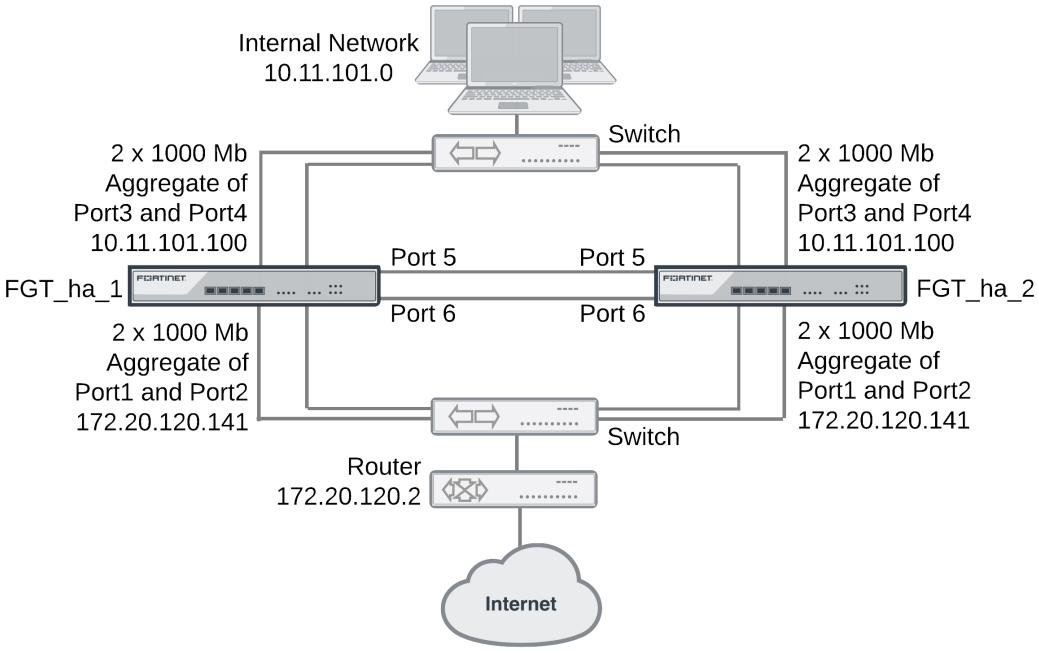
FGCP HA with 802.3ad aggregated interfaces

On FortiGate models that support it you can use 802.3ad link aggregation to combine two or more interfaces into a single aggregated interface. 802.3ad Link Aggregation and it's management protocol, Link Aggregation Control Protocol (LACP) are a method for combining multiple physical links into a single logical link.This increases both potential throughput and network resiliency. Using LACP, traffic is distributed among the physical interfaces in the link, potentially resulting in increased performance.

This example describes how to configure an HA cluster consisting of two FortiGate units with two aggregated 1000 Mb connections to the Internet using port1 and port2 and two aggregated 1000 Mb connections to the internal network using port3 and port4. The aggregated interfaces are also configured as HA monitored interfaces.

Each of the aggregate links connects to a different switch. Each switch is configured for link aggregation (2x1000Mb).

Example cluster with aggregate interfaces



HA interface monitoring, link failover, and 802.3ad aggregation

When monitoring the aggregated interface, HA interface monitoring treats the aggregated link as a single interface and does not monitor the individual physical interfaces in the link. HA interface monitoring registers the link to have failed only if all the physical interfaces in the link have failed. If only some of the physical interfaces in the link fail or become disconnected, HA considers the link to be operating normally.

HA MAC addresses and 802.3ad aggregation

If a configuration uses the Link Aggregate Control Protocol (LACP) (either passive or active), LACP is negotiated over all of the interfaces in any link. For a standalone FortiGate unit, the FortiGate LACP implementation uses the MAC address of the first interface in the link to uniquely identify that link. For example, a link consisting of port1 and port2 interfaces would have the MAC address of port1.

In an HA cluster, HA changes the MAC addresses of the cluster interfaces to virtual MAC addresses. An aggregate interface in a cluster acquires the virtual MAC address that would have been acquired by the first interface in the aggregate.

Link aggregation, HA failover performance, and HA mode

To operate an active-active or active-passive cluster with aggregated interfaces and for best performance of a cluster with aggregated interfaces, the switches used to connect the cluster unit aggregated interfaces together should support configuring multiple Link Aggregation (LAG) groups.

For example, the cluster shown above should be configured into two LAG groups on the external switch: one for the port1 and port2 aggregated interface of FGT_ha_1 and a second one for the port1 and port2 aggregate interface of FGT_ha_2. You should also be able to do the same on the internal switch for the port3 and port4 aggregated interfaces of each cluster unit.

As a result, the subordinate unit aggregated interfaces would participate in LACP negotiation while the cluster is operating. In an active-active mode cluster, packets could be redirected to the subordinate unit interfaces. As well, in active-active or active-passive mode, after a failover the subordinate unit can become a primary unit without having to perform LACP negotiation before it can process traffic. Performing LACP negotiation causes a minor failover delay.

However if you cannot configure multiple LAG groups on the switches, due to the primary and subordinate unit interfaces having the same MAC address, the switch will put all of the interfaces into the same LAG group which would disrupt the functioning of the cluster. To prevent this from happening, you must change the FortiGate aggregated interface configuration to prevent subordinate units from participating in LACP negotiation.

For example, use the following command to prevent subordinate units from participating in LACP negotiation with an aggregate interface named Port1_Port2:

```
config system interface
   edit Port1_Port2
      set lacp-ha-slave disable
   end
```

As a result of this setting, subordinate unit aggregated interfaces cannot accept packets. This means that you cannot operate the cluster in active-active mode because in active-active mode the subordinate units must be able to receive and process packets. Also, failover may take longer because after a failover the subordinate unit has to perform LACP negotiation before being able to process network traffic.

Also, it may also be necessary to configure the switch to use Passive or even Static mode for LACP to prevent the switch from sending packets to the subordinate unit interfaces, which won't be able to process them.

Finally, in some cases depending on the LACP configuration of the switches, you may experience delayed failover if the FortiGate LACP configuration is not compatible with the switch LACP configuration. For example, in some cases setting the FortiGate LACP mode to static reduces the failover delay because the FortiGate unit does not perform LACP negotiation. However there is a potential problem with this configuration because static LACP does not send periodic LAC Protocol Data Unit (LACPDU) packets to test the connections. So a non-physical failure (for example, if a device is not responding because its too busy) may not be detected and packets could be lost or delayed.

General configuration steps

The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate units are running the same FortiOS firmware build and are set to the factory default configuration.

General configuration steps

1. Apply licenses to the FortiGate units to become the cluster.
2. Configure the FortiGate units for HA operation.
   - Change each unit's host name.
   - Configure HA.
2. Connect the cluster to the network.
3. View cluster status.
4. Add basic configuration settings and configure the aggregated interfaces.

- Add a password for the admin administrative account.
- Add the aggregated interfaces.
- Disable `lacp-ha-slave` so that the subordinate unit does not send LACP packets.
- Add a default route.

You could also configure aggregated interfaces in each FortiGate unit before the units form a cluster.

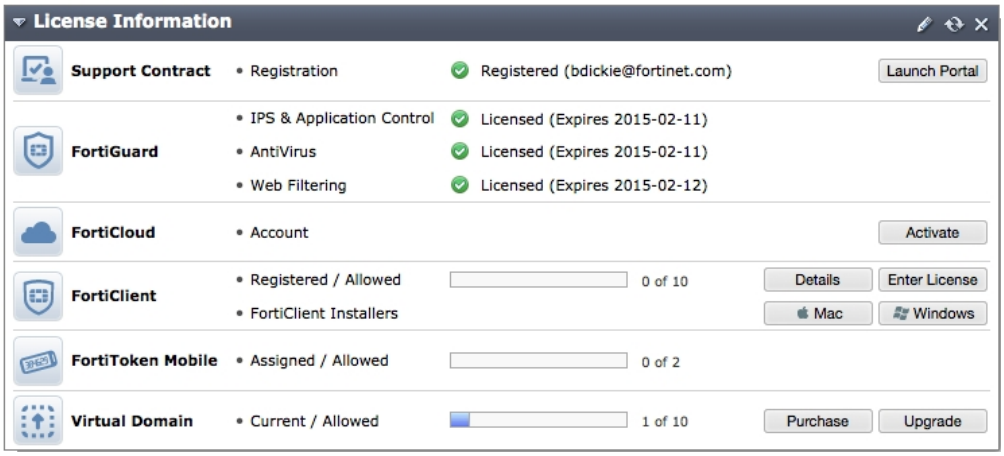
5. Configure HA port monitoring for the aggregated interfaces.

Configuring active-passive HA cluster that includes aggregated interfaces - web-based manager

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Select **OK**.
6. Go to **System > Config > HA** and change the following settings.

Mode	Active-Passive
Group Name	example5.com
Password	HA_pass_5
Heartbeat Interface	

	Enable	Priority
port5	Select	50
port6	Select	50

Since port3 and port4 will be used for an aggregated interface, you must change the HA heartbeat configuration to not use those interfaces.

7. Select **OK**.

   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

   - port1 interface virtual MAC: `00-09-0f-09-00-00`
   - port10 interface virtual MAC: `00-09-0f-09-00-01`
   - port11 interface virtual MAC: `00-09-0f-09-00-02`
   - port12 interface virtual MAC: `00-09-0f-09-00-03`
   - port13 interface virtual MAC: `00-09-0f-09-00-04`
   - port14 interface virtual MAC: `00-09-0f-09-00-05`
   - port15 interface virtual MAC: `00-09-0f-09-00-06`
   - port16 interface virtual MAC: `00-09-0f-09-00-07`
   - port17 interface virtual MAC: `00-09-0f-09-00-08`
   - port18 interface virtual MAC: `00-09-0f-09-00-09`
   - port19 interface virtual MAC: `00-09-0f-09-00-0a`
   - port2 interface virtual MAC: `00-09-0f-09-00-0b`
   - port20 interface virtual MAC: `00-09-0f-09-00-0c`
   - port3 interface virtual MAC: `00-09-0f-09-00-0d`
   - port4 interface virtual MAC: `00-09-0f-09-00-0e`
   - port5 interface virtual MAC: `00-09-0f-09-00-0f`
   - port6 interface virtual MAC: `00-09-0f-09-00-10`
   - port7 interface virtual MAC: `00-09-0f-09-00-11`
   - port8 interface virtual MAC: `00-09-0f-09-00-12`
   - port9 interface virtual MAC: `00-09-0f-09-00-13`

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

   You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

   ```
   get hardware nic port1
   .
   .
   .
   MAC: 00:09:0f:09:00:00
   ```

```
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

7. Power off the first FortiGate unit.
8. Repeat these steps for the second FortiGate unit.
   Set the second FortiGate unit host name to:

New Name	FGT_ha_2

To connect the cluster to the network

1. Connect the port1 and port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
   Configure the switch so that the port1 and port2 of FGT_ha_1 make up an aggregated interface and port1 and port2 of FGT_ha_2 make up a second aggregated interface.
2. Connect the port3 and port4 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
   Configure the switch so that the port3 and port4 of FGT_ha_1 make up an aggregated interface and port3 and port4 of FGT_ha_2 make up another aggregated interface.
3. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port5 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.
   The units negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete, the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster.

1. View the system dashboard.
   The System Information dashboard widget shows the **Cluster Name** (example5.com) and the host names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.
2. Go to **System > Config > HA** to view the cluster members list.
   The list shows two cluster units, their host names, their roles in the cluster, and their priorities. You can use this list to confirm that the cluster is operating normally.

To troubleshoot the cluster configuration

See FGCP HA with 802.3ad aggregated interfaces on page 1359 to troubleshoot the cluster.

To add basic configuration settings and the aggregate interfaces

Use the following steps to add a few basic configuration settings.

1. Log into the cluster web-based manager.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.
5. Select **OK**.
6. Go to **Router > Static** > Static Routes and temporarily delete the default route.
   You cannot add an interface to a aggregated interface if any settings (such as the default route) are configured for it.
7. Go to **System > Network > Interfaces** and select **Create New** to add the aggregate interface to connect to the Internet.
8. Set **Type** to **802.3ad Aggregate** and configure the aggregate interface to be connected to the Internet:

Name	Port1_Port2
Physical Interface Members	port1, port2
IP/Network Mask	172.20.120.141/24

9. Select **OK**.
10. Select **Create New** to add the aggregate interface to connect to the internal network.
11. Set **Type** to **802.3ad Aggregate** and configure the aggregate interface to be connected to the Internet:

Name	Port3_Port4
Physical Interface Members	port3, port4
IP/Netmask	10.11.101.100/24
Administrative Access	HTTPS, PING, SSH

12. Select **OK**.
    The virtual MAC addresses of the FortiGate interfaces change to the following. Note that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:
    - port1 interface virtual MAC: `00-09-0f-09-00-00`
    - port10 interface virtual MAC: `00-09-0f-09-00-01`
    - port11 interface virtual MAC: `00-09-0f-09-00-02`
    - port12 interface virtual MAC: `00-09-0f-09-00-03`
    - port13 interface virtual MAC: `00-09-0f-09-00-04`
    - port14 interface virtual MAC: `00-09-0f-09-00-05`
    - port15 interface virtual MAC: `00-09-0f-09-00-06`
    - port16 interface virtual MAC: `00-09-0f-09-00-07`
    - port17 interface virtual MAC: `00-09-0f-09-00-08`

- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

13. Connect to the CLI and enter the following command to disable sending LACP packets from the subordinate unit:

```
config system interface
   edit Port1_Port2
      set lacp-ha-slave disable
   next
   edit Port3_Port4
      set lacp-ha-slave disable
end
```

14. Go to **Router > Static > Static Routes**.
15. Add the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	Port1_Port2
Distance	10

16. Select **OK**.

To configure HA port monitoring for the aggregate interfaces

1. Go to **System > Config > HA**.
2. In the cluster members list, edit the primary unit.
3. Configure the following port monitoring for the aggregate interfaces:

	Port Monitor
Port1_Port2	Select
Port3_Port4	Select

4. Select **OK**.

Configuring active-passive HA cluster that includes aggregate interfaces - CLI

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
2. Install any third-party certificates on the FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. Change the host name for this FortiGate unit:
   ```
   config system global
      set hostname FGT_ha_1
   end
   ```
4. Configure HA settings.
   ```
   config system ha
      set mode a-p
      set group-name example5.com
      set password HA_pass_5
      set hbdev port5 50 port6 50
   end
   ```
   Since port3 and port4 will be used for an aggregated interface, you must change the HA heartbeat configuration.

   The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

   - port1 interface virtual MAC: `00-09-0f-09-00-00`
   - port10 interface virtual MAC: `00-09-0f-09-00-01`
   - port11 interface virtual MAC: `00-09-0f-09-00-02`
   - port12 interface virtual MAC: `00-09-0f-09-00-03`
   - port13 interface virtual MAC: `00-09-0f-09-00-04`
   - port14 interface virtual MAC: `00-09-0f-09-00-05`
   - port15 interface virtual MAC: `00-09-0f-09-00-06`
   - port16 interface virtual MAC: `00-09-0f-09-00-07`
   - port17 interface virtual MAC: `00-09-0f-09-00-08`
   - port18 interface virtual MAC: `00-09-0f-09-00-09`
   - port19 interface virtual MAC: `00-09-0f-09-00-0a`
   - port2 interface virtual MAC: `00-09-0f-09-00-0b`
   - port20 interface virtual MAC: `00-09-0f-09-00-0c`
   - port3 interface virtual MAC: `00-09-0f-09-00-0d`
   - port4 interface virtual MAC: `00-09-0f-09-00-0e`
   - port5 interface virtual MAC: `00-09-0f-09-00-0f`
   - port6 interface virtual MAC: `00-09-0f-09-00-10`
   - port7 interface virtual MAC: `00-09-0f-09-00-11`
   - port8 interface virtual MAC: `00-09-0f-09-00-12`
   - port9 interface virtual MAC: `00-09-0f-09-00-13`

   To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP

table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

4. Repeat these steps for the other FortiGate unit.

   Set the other FortiGate unit host name to:

```
config system global
   set hostname FGT_ha_2
end
```

To connect the cluster to the network

1. Connect the port1 and port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.

   Configure the switch so that the port1 and port2 of FGT_ha_1 make up an aggregated interface and port1 and port2 of FGT_ha_2 make up another aggregated interface.
2. Connect the port3 and port4 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.

   Configure the switch so that the port3 and port4 of FGT_ha_1 make up an interfaced and port3 and port4 of FGT_ha_2 make up another aggregated interface.
3. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port5 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.

   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view cluster status from the CLI.

1. Log into the CLI.
2. Enter `get system status` to verify the HA status of the cluster unit that you logged into. Look for the following information in the command output.

`Current HA mode: a-a, master`	The cluster units are operating as a cluster and you have connected to the primary unit.
`Current HA mode: a-a, backup`	The cluster units are operating as a cluster and you have connected to a subordinate unit.
`Current HA mode: standalone`	The cluster unit is not operating in HA mode

3. Enter the following command to confirm the HA configuration of the cluster:

```
get system ha status
   Model: XXXX
   Mode: a-a
   Group: 0
   Debug: 0
   ses_pickup: disable
   Master:128 FGT_ha_2 FG600B3908600825 0
   Slave :128 FGT_ha_1 FG600B3908600705 1
   number of vcluster: 1
   vcluster 1: work 169.254.0.1
   Master:0 FG600B3908600825
   Slave :1 FG600B3908600705
```

The command output shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this command to confirm that the cluster is operating normally. For example, if the command shows only one cluster unit then the other unit has left the cluster for some reason.

To troubleshoot the cluster configuration

See FGCP HA with 802.3ad aggregated interfaces on page 1359 to troubleshoot the cluster.

To add basic configuration settings and the aggregate interfaces

Use the following steps to add a few basic configuration settings and the aggregate interfaces.

1. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <psswrd>
end
```

2. Temporarily delete the default route.

   You cannot add an interface to an aggregate interface if any settings (such as the default route) are configured for it. In this example the index of the default route is 1.

```
config router static
   delete 1
end
```

3. Add the aggregate interfaces:

```
config system interface
   edit Port1_Port2
      set type aggregate
      set lacp-ha-slave disable
      set member port1 port2
```

```
      set ip 172.20.120.141/24
      set vdom root
    next
    edit Port3_Port4
      set type aggregate
      set lacp-ha-slave disable
      set member port3 port4
      set ip 10.11.101.100/24
      set vdom root
end
```

The virtual MAC addresses of the FortiGate interfaces change to the following. Note that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

4. Add the default route.

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 172.20.120.2
    set device Port1_Port2
end
```

To configure HA port monitoring for the aggregate interfaces

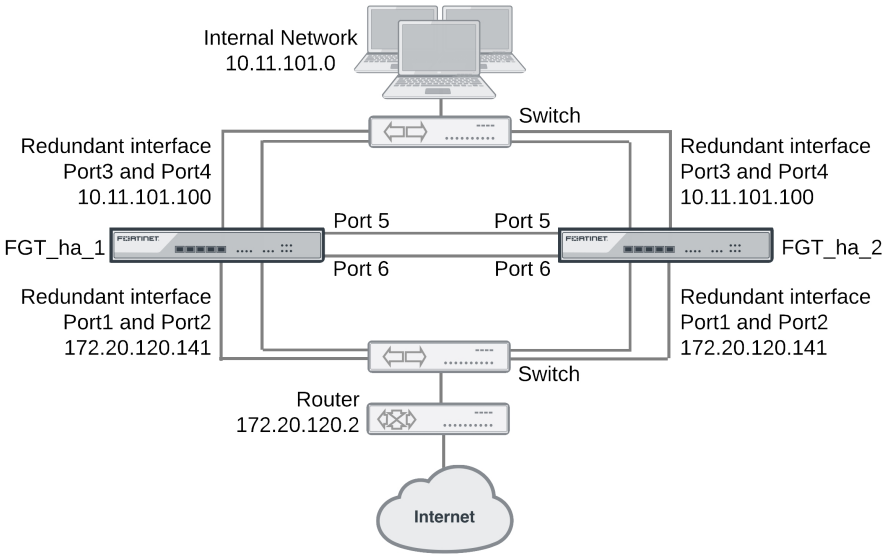
1. Configure HA port monitoring for the aggregate interfaces.

```
config system ha
  set monitor Port1_Port2 Port3_Port4
end
```

Example HA and redundant interfaces

On FortiGate models that support it you can combine two or more interfaces into a single redundant interface. A redundant interface consists of two or more physical interfaces. Traffic is processed by the first physical interface in the redundant interface. If that physical interface fails, traffic fails over to the next physical interface. Redundant interfaces don't have the benefit of improved performance that aggregate interfaces can have, but they do provide failover if a physical interface fails or is disconnected.

Example cluster with a redundant interfaces



This example describes how to configure an HA cluster consisting of two FortiGate units with a a redundant interface connection to the Internet and to an internal network. The connection to the Internet uses port1 and port2. The connection to the internal network uses port3 and port4. The HA heartbeat uses port5 and port6.

The redundant interfaces are also configured as HA monitored interfaces.

HA interface monitoring, link failover, and redundant interfaces

HA interface monitoring monitors the redundant interface as a single interface and does not monitor the individual physical interfaces in the redundant interface. HA interface monitoring registers the redundant interface to have failed only if all the physical interfaces in the redundant interface have failed. If only some of the physical interfaces in the redundant interface fail or become disconnected, HA considers the redundant interface to be operating normally.

HA MAC addresses and redundant interfaces

For a standalone FortiGate unit a redundant interface has the MAC address of the first physical interface added to the redundant interface configuration. A redundant interface consisting of port1 and port2 would have the MAC address of port1.

In an HA cluster, HA changes the MAC addresses of the cluster interfaces to virtual MAC addresses. A redundant interface in a cluster acquires the virtual MAC address that would have been acquired by the first physical interface added to the redundant interface configuration.

Connecting multiple redundant interfaces to one switch while operating in active-passive HA mode

HA assigns the same virtual MAC addresses to the subordinate unit interfaces as are assigned to the corresponding primary unit interfaces. Consider a cluster of two FortiGate units operating in active-passive mode with a redundant interface consisting of port1 and port2. You can connect multiple redundant interfaces to the same switch if you configure the switch so that it defines multiple separate redundant interfaces and puts the redundant interfaces of each cluster unit into separate redundant interfaces. In this configuration, each cluster unit forms a separate redundant interface with the switch.

However, if the switch is configured with a single four-port redundant interface configuration, because the same MAC addresses are being used by both cluster units, the switch adds all four interfaces (port1 and port2 from the primary unit and port1 and port2 from the subordinate unit) to the same redundant interface.

To avoid unpredictable results, when you connect a switch to multiple redundant interfaces in an active-passive cluster you should configure separate redundant interfaces on the switch; one for each cluster unit.

Connecting multiple redundant interfaces to one switch while operating in active-active HA mode

In an active-active cluster, all cluster units send and receive packets. To operate a cluster with redundant interfaces in active-active mode, with multiple redundant interfaces connected to the same switch, you must separate the redundant interfaces of each cluster unit into different redundant interfaces on the connecting switch.

General configuration steps

The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate units are running the same FortiOS firmware build and are set to the factory default configuration.

General configuration steps

1. Apply licenses to the FortiGate units to become the cluster.
2. Configure the FortiGate units for HA operation.
   - Change each unit's host name.
   - Configure HA.
2. Connect the cluster to the network.
3. View cluster status.
4. Add basic configuration settings and configure the redundant interfaces.
   - Add a password for the admin administrative account.
   - Add the redundant interfaces.
   - Add a default route.

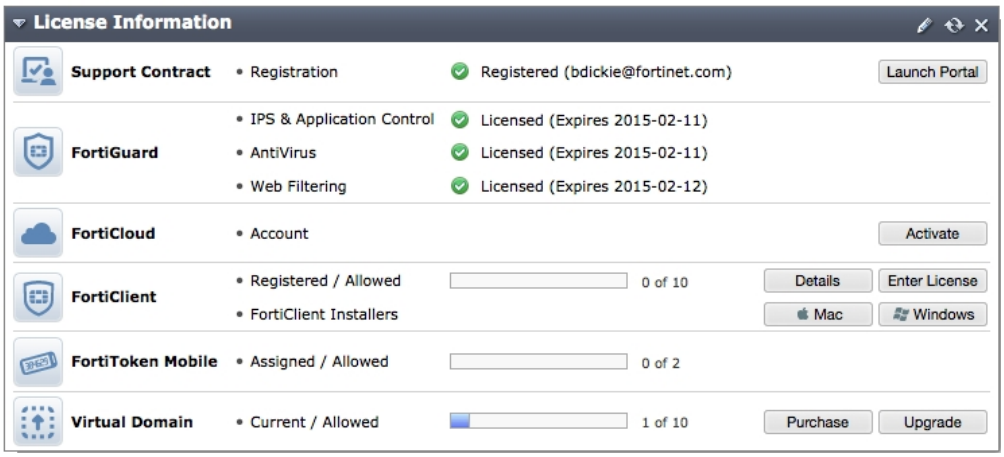
   You could also configure redundant interfaces in each FortiGate unit before they form a cluster.
5. Configure HA port monitoring for the redundant interfaces.

Configuring active-passive HA cluster that includes redundant interfaces - web-based manager

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Select **OK**.
6. Go to **System > Config > HA** and change the following settings.

Mode	Active-Passive	
Group Name	example6.com	
Password	HA_pass_6	
Heartbeat Interface		
	Enable	**Priority**
port5	Select	50
port6	Select	50

   Since port3 and port4 will be used for a redundant interface, you must change the HA heartbeat configuration.

7. Select **OK**.

The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

7. Power off the first FortiGate unit.
8. Repeat these steps for the second FortiGate unit.

   Set the second FortiGate unit host name to:

New Name	FGT_ha_2

To connect the cluster to the network

1. Connect the port1 and port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
   Configure the switch so that the port1 and port2 of FGT_ha_1 make up a redundant interface and port1 and port2 of FGT_ha_2 make up another redundant interface.
2. Connect the port3 and port4 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
   Configure the switch so that the port3 and port4 of FGT_ha_1 make up a redundant interface and port3 and port4 of FGT_ha_2 make up another redundant interface.
3. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port5 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster.

1. View the system dashboard.
   The System Information dashboard widget shows the **Cluster Name** (example5.com) and the host names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.
2. Go to **System > Config > HA** to view the cluster members list.
   The list shows two cluster units, their host names, their roles in the cluster, and their priorities. You can use this list to confirm that the cluster is operating normally.

To troubleshoot the cluster configuration

See Example HA and redundant interfaces on page 1371 to troubleshoot the cluster.

To add basic configuration settings and the redundant interfaces

Use the following steps to add a few basic configuration settings.

1. Log into the cluster web-based manager.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.
5. Select **OK**.
6. Go to **Router > Static > Static Routes** and temporarily delete the default route.

You cannot add an interface to a redundant interface if any settings (such as the default route) are configured for it.

7. Go to **System > Network > Interfaces** and select **Create New** to add the redundant interface to connect to the Internet.
8. Set **Type** to **Redundant Interface** and configure the redundant interface to be connected to the Internet:

Name	Port1_Port2
Physical Interface Members	port1, port2
IP/Netmask	172.20.120.141/24

9. Select **OK**.
10. Select **Create New** to add the redundant interface to connect to the internal network.
11. Set **Type** to **Redundant Interface** and configure the redundant interface to be connected to the Internet:

Name	Port3_Port4
Physical Interface Members	port3, port4
IP/Netmask	10.11.101.100/24
Administrative Access	HTTPS, PING, SSH

12. Select **OK**.
    The virtual MAC addresses of the FortiGate interfaces change to the following. Note that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`

- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

13. Go to **Router > Static > Static Routes**.
14. Add the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	Port1_Port2
Distance	10

15. Select **OK**.

To configure HA port monitoring for the redundant interfaces

1. Go to **System > Config > HA**.
2. In the cluster members list, edit the primary unit.
3. Configure the following port monitoring for the redundant interfaces:

	Port Monitor
Port1_Port2	Select
Port3_Port4	Select

4. Select **OK**.

Configuring active-passive HA cluster that includes redundant interfaces - CLI

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. Change the host name for this FortiGate unit:

```
config system global
   set hostname FGT_ha_1
end
```

4. Configure HA settings.

```
config system ha
   set mode a-p
   set group-name example6.com
   set password HA_pass_6
   set hbdev port5 50 port6 50
end
```

Since port3 and port4 will be used for a redundant interface, you must change the HA heartbeat configuration.

The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

4. Repeat these steps for the other FortiGate unit.
   Set the other FortiGate unit host name to:

```
config system global
   set hostname FGT_ha_2
end
```

To connect the cluster to the network

1. Connect the port1 and port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
   Configure the switch so that the port1 and port2 of FGT_ha_1 make up a redundant interface and port1 and port2 of FGT_ha_2 make up another redundant interface.
2. Connect the port3 and port4 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
   Configure the switch so that the port3 and port4 of FGT_ha_1 make up a redundant interface and port3 and port4 of FGT_ha_2 make up another redundant interface.
3. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
4. Connect the port5 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
5. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally takes less than a minute.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view cluster status from the CLI.

1. Log into the CLI.
2. Enter `get system status` to verify the HA status of the cluster unit that you logged into.Look for the following information in the command output.

`Current HA mode: a-a, master`	The cluster units are operating as a cluster and you have connected to the primary unit.
`Current HA mode: a-a, backup`	The cluster units are operating as a cluster and you have connected to a subordinate unit.
`Current HA mode: standalone`	The cluster unit is not operating in HA mode

3. Enter the following command to confirm the HA configuration of the cluster:

```
get system ha status
   Model: XXXX
   Mode: a-a
   Group: 0
   Debug: 0
   ses_pickup: disable
   Master:128 FGT_ha_2 FG600B3908600825 0
   Slave :128 FGT_ha_1 FG600B3908600705 1
   number of vcluster: 1
   vcluster 1: work 169.254.0.1
   Master:0 FG600B3908600825
```

```
Slave :1 FG600B3908600705
```

The command output shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this command to confirm that the cluster is operating normally. For example, if the command shows only one cluster unit then the other unit has left the cluster for some reason.

To troubleshoot the cluster configuration

See Example HA and redundant interfaces on page 1371 to troubleshoot the cluster.

To add basic configuration settings and the redundant interfaces

Use the following steps to add a few basic configuration settings and the redundant interfaces.

1. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <psswrd>
end
```

2. Temporarily delete the default route.

   You cannot add an interface to a redundant interface if any settings (such as the default route) are configured for it. In this example the index of the default route is 1.

```
config router static
   delete 1
end
```

3. Add the redundant interfaces:

```
config system interface
   edit Port1_Port2
      set type redundant
      set member port1 port2
      set ip 172.20.120.141/24
      set vdom root
   next
   edit Port3_Port4
      set type redundant
      set member port3 port4
      set ip 10.11.101.100/24
      set vdom root
end
```

   The virtual MAC addresses of the FortiGate interfaces change to the following. Note that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:

   - port1 interface virtual MAC: `00-09-0f-09-00-00`
   - port10 interface virtual MAC: `00-09-0f-09-00-01`
   - port11 interface virtual MAC: `00-09-0f-09-00-02`
   - port12 interface virtual MAC: `00-09-0f-09-00-03`
   - port13 interface virtual MAC: `00-09-0f-09-00-04`
   - port14 interface virtual MAC: `00-09-0f-09-00-05`
   - port15 interface virtual MAC: `00-09-0f-09-00-06`
   - port16 interface virtual MAC: `00-09-0f-09-00-07`

- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

4. Add the default route.

```
config router static
   edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 172.20.120.2
      set device Port1_Port2
end
```

To configure HA port monitoring for the redundant interfaces

1. Configure HA port monitoring for the redundant interfaces.

```
config system ha
   set monitor Port1_Port2 Port3_Port4
end
```

Troubleshooting HA clusters

This section describes some HA clustering troubleshooting techniques.

Ignoring hardware revisions

Many FortiGate platforms have gone through multiple hardware versions and in some cases the hardware changes prevent cluster formation. If you run into this problem you can use the following command on each FortiGate to cause the cluster to ignore different hardware versions:

```
execute ha ignore-hardware-revision enable
```

This command is only available on FortiGates that have had multiple hardware revisions.

By default the command is set to prevent cluster formation between FortiGates with different hardware revisions. You can enter the following command to view its status:

```
execute ha ignore-hardware-revision status
```

Usually the incompatibility is caused by different hardware versions having different hard disks and enabling this command disables each FortiGate's hard disks. As a result of disabling hard disks the cluster will not support logging to the hard disk or WAN Optimization.

If the FortiGates do have compatible hardware versions or if you want to run a FortiGate in standalone mode you can enter the following command to disable ignoring the hardware revision and enable the hard disks:

```
execute ha ignore-hardware-revision disable
```

Affected models include but are not limited to:

- FortiGate-100D
- FortiGate-300C
- FortiGate-600C
- FortiGate-800C
- FortiGate-80C and FortiWiFi-80C
- FortiGate-60C

Its possible that a cluster will not form because the disk partition sizes of the cluster units are different. You can use the `diagnose sys ha showcsum 1 system | grep storage` command to check the disk storage checksum of each cluster unit. If the checksums are different then contact Fortinet support for help in setting up compatible storage partitions.

Before you set up a cluster

Before you set up a cluster ask yourself the following questions about the FortiGate units that you are planning to use to create a cluster.

1. Do all the FortiGate units have the same hardware configuration? Including the same hard disk configuration and the same AMC cards installed in the same slots?
2. Do all FortiGate units have the same firmware build?
3. Are all FortiGate units set to the same operating mode (NAT or Transparent)?
4. Are all the FortiGate units operating in single VDOM mode?
5. If the FortiGate units are operating in multiple VDOM mode do they all have the same VDOM configuration?

In some cases you may be able to form a cluster if different FortiGate units have different firmware builds, different VDOM configurations, and are in different operating modes. However, if you encounter problems they may be resolved by installing the same firmware build on each unit, and give them the same VDOM configuration and operating mode.

Troubleshooting the initial cluster configuration

This section describes how to check a cluster when it first starts up to make sure that it is configured and operating correctly. This section assumes you have already configured your HA cluster.

To verify that a cluster can process traffic and react to a failure

1. Add a basic security policy configuration and send network traffic through the cluster to confirm connectivity.

   For example, if the cluster is installed between the Internet and an internal network, set up a basic internal to external security policy that accepts all traffic. Then from a PC on the internal network, browse to a website on the Internet or ping a server on the Internet to confirm connectivity.
2. From your management PC, set ping to continuously ping the cluster, and then start a large download, or in some other way establish ongoing traffic through the cluster.
3. While traffic is going through the cluster, disconnect the power from one of the cluster units.

   You could also shut down or restart a cluster unit.

   Traffic should continue with minimal interruption.

4. Start up the cluster unit that you disconnected.
   The unit should re-join the cluster with little or no affect on traffic.
5. Disconnect a cable for one of the HA heartbeat interfaces.
   The cluster should keep functioning, using the other HA heartbeat interface.
6. If you have port monitoring enabled, disconnect a network cable from a monitored interface.
   Traffic should continue with minimal interruption.

To verify the cluster configuration - web-based manager

1. Log into the cluster web-based manager.
2. Check the system dashboard to verify that the System Information widget displays all of the cluster units.
3. Check the cluster member graphic to verify that the correct cluster unit interfaces are connected.
4. Go to **System > Config > HA** and verify that all of the cluster units are displayed on the cluster members list.
5. From the cluster members list, edit the primary unit (master) and verify the cluster configuration is as expected.

To troubleshoot the cluster configuration - web-based manager

1. Connect to each cluster unit web-based manager and verify that the HA configurations are the same.
2. To connect to each web-based manager, you may need to disconnect some units from the network to connect to the other if the units have the same IP address.
3. If the configurations are the same, try re-entering the cluster **Password** on each cluster unit in case you made an error typing the password when configuring one of the cluster units.
4. Check that the correct interfaces of each cluster unit are connected.
   Check the cables and interface LEDs.

   Use the Unit Operation dashboard widget, system network interface list, or cluster members list to verify that each interface that should be connected actually is connected.

   If Link is down re-verify the physical connection. Try replacing network cables or switches as required.

To verify the cluster configuration - CLI

1. Log into each cluster unit CLI.
   You can use the console connection if you need to avoid the problem of units having the same IP address.
2. Enter the command `get system status`.
   Look for the following information in the command output.

`Current HA mode: a-a, master`	The cluster units are operating as a cluster and you have connected to the primary unit.
`Current HA mode: a-a, backup`	The cluster units are operating as a cluster and you have connected to a subordinate unit.
`Current HA mode: standalone`	The cluster unit is not operating in HA mode

3. Verify that the `get system ha status` command displays all of the cluster units.
4. Enter the `get system ha` command to verify that the HA configuration is correct and the same for each cluster unit.

To troubleshoot the cluster configuration - CLI

1. Try using the following command to re-enter the cluster password on each cluster unit in case you made an error typing the password when configuring one of the cluster units.

```
config system ha
   set password <password>
end
```

2. Check that the correct interfaces of each cluster unit are connected.

   Check the cables and interface LEDs.

   Use `get hardware nic <interface_name>` command to confirm that each interface is connected. If the interface is connected the command output should contain a `Link: up` entry similar to the following:

```
get hardware nic port1
.
.
.
Link: up
.
.
.
```

   If Link is down, re-verify the physical connection. Try replacing network cables or switches as required.

More troubleshooting information

Much of the information in this HA guide can be useful for troubleshooting HA clusters. Here are some links to sections with more information.

- If sessions are lost after a failover you may need to change route-ttl to keep synchronized routes active longer. See Controlling how the FGCP synchronizes kernel routing table updates on page 1481.
- To control which cluster unit becomes the primary unit, you can change the device priority and enable override. See An introduction to the FGCP on page 1270.
- Changes made to a cluster can be lost if override is enabled. See An introduction to the FGCP on page 1270.
- In some cases, age differences among cluster units result in the wrong cluster unit becoming the primary unit. For example, if a cluster unit set to a high priority reboots, that unit will have a lower age than other cluster units. You can resolve this problem by resetting the age of one or more cluster units. See An introduction to the FGCP on page 1270. You can also adjust how sensitive the cluster is to age differences. This can be useful if large age differences cause problems. SeeAn introduction to the FGCP on page 1270 and An introduction to the FGCP on page 1270.
- If one of the cluster units needs to be serviced or removed from the cluster for other reasons, you can do so without affecting the operation of the cluster. See Disconnecting a cluster unit from a cluster on page 1451.
- The web-based manager and CLI will not allow you to configure HA if you have enabled FGSP HA. See FortiGate Session Life Support Protocol (FGSP) on page 1535.
- The web-based manager and CLI will not allow you to configure HA if one or more FortiGate unit interfaces is configured as a PPTP or L2TP client.

- The FGCP is compatible with DHCP and PPPoE but care should be taken when configuring a cluster that includes a FortiGate interface configured to get its IP address with DHCP or PPPoE. Fortinet recommends that you turn on DHCP or PPPoE addressing for an interface after the cluster has been configured. See An introduction to the FGCP on page 1270.
- Some third-party network equipment may prevent HA heartbeat communication, resulting in a failure of the cluster or the creation of a split brain scenario. For example, some switches use packets with the same Ethertype as HA heartbeat packets use for internal functions and when used for HA heartbeat communication the switch generates CRC errors and the packets are not forwarded. See Heartbeat packet Ethertypes on page 1461.
- Very busy clusters may not be able to send HA heartbeat packets quickly enough, also resulting in a split brain scenario. You may be able to resolve this problem by modifying HA heartbeat timing. See Modifying heartbeat timing on page 1462.
- Very busy clusters may suffer performance reductions if session pickup is enabled. If possible you can disable this feature to improve performance. If you require session pickup for your cluster, several options are available for improving session pickup performance. See Improving session synchronization performance on page 1496.
- If it takes longer than expected for a cluster to failover you can try changing how the primary unit sends gratuitous ARP packets. See Changing how the primary unit sends gratuitous ARP packets after a failover on page 1465.
- You can also improve failover times by configuring the cluster for subsecond failover. See Subsecond failover on page 1491 and Failover performance on page 1506.
- When you first put a FortiGate unit in HA mode you may loose connectivity to the unit. This occurs because HA changes the MAC addresses of all FortiGate unit interfaces, including the one that you are connecting to. The cluster MAC addresses also change if you change the some HA settings such as the cluster group ID. The connection will be restored in a short time as your network and PC updates to the new MAC address. To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.
- Since HA changes all cluster unit MAC addresses, if your network uses MAC address filtering you may have to make configuration changes to account for the HA MAC addresses.
- A network may experience packet loss when two FortiGate HA clusters have been deployed in the same broadcast domain. Deploying two HA clusters in the same broadcast domain can result in packet loss because of MAC address conflicts. The packet loss can be diagnosed by pinging from one cluster to the other or by pinging both of the clusters from a device within the broadcast domain. You can resolve the MAC address conflict by changing the HA Group ID configuration of the two clusters. The HA Group ID is sometimes also called the Cluster ID. See Diagnosing packet loss with two FortiGate HA clusters in the same broadcast domain on page 1469.
- A network may experience packet loss when two FortiGate HA clusters have been deployed in the same broadcast domain. Deploying two HA clusters in the same broadcast domain can result in packet loss because of MAC address conflicts. The packet loss can be diagnosed by pinging from one cluster to the other or by pinging both of the clusters from a device within the broadcast domain. You can resolve the MAC address conflict by changing the HA Group ID configuration of the two clusters. The HA Group ID is sometimes also called the Cluster ID. See Diagnosing packet loss with two FortiGate HA clusters in the same broadcast domain on page 1469.
- The cluster CLI displays `slave is not in sync` messages if there is a synchronization problem between the primary unit and one or more subordinate units. See How to diagnose HA out of sync messages on page 1479.
- If you have configured dynamic routing and the new primary unit takes too long to update its routing table after a failover you can configure graceful restart and also optimize how routing updates are synchronized. See Configuring graceful restart for dynamic routing failover on page 1482 and Controlling how the FGCP synchronizes kernel routing table updates on page 1481.
- Some switches may not be able to detect that the primary unit has become a subordinate unit and will keep sending packets to the former primary unit. This can occur after a link failover if the switch does not detect the failure and

does not clear its MAC forwarding table. See Updating MAC forwarding tables when a link failover occurs on page 1489.

- If a link not directly connected to a cluster unit (for example, between a switch connected to a cluster interface and the network) fails you can enable remote link failover to maintain communication. See Remote link failover on page 1491.
- If you find that some cluster units are not running the same firmware build you can reinstall the correct firmware build on the cluster to upgrade all cluster units to the same firmware build. See Synchronizing the firmware build running on a new cluster unit on page 1440.

Virtual clusters

This chapter provides an introduction to virtual clustering and also contains general procedures and configuration examples that describe how to configure FortiGate HA virtual clustering.

Virtual clustering overview

Virtual clustering is an extension of the FGCP for a cluster of 2 FortiGate units operating with multiple VDOMS enabled. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a VDOM operating on two different cluster units. You can also operate virtual clustering in active-active mode to use HA load balancing to load balance sessions between cluster units. Alternatively, by distributing VDOM processing between the two cluster units you can also configure virtual clustering to provide load balancing by distributing sessions for different VDOMs to each cluster unit.

The figure below shows an example virtual cluster configuration consisting of two FortiGate units. The virtual cluster has two virtual domains, root and Eng_vdm.

The root virtual domain includes the port1 and port2 interfaces. The Eng_vdm virtual domain includes the port5 and port6 interfaces. The port3 and port4 interfaces (not shown in the diagram) are the HA heartbeat interfaces.

FortiGate virtual clustering is limited to a cluster of 2 FortiGate units with multiple VDOMs enabled. If you want to create a cluster of more than 2 FortiGate units operating with multiple VDOMS you could consider other solutions that either do not include multiple VDOMs in one cluster or employ a feature such as standalone session synchronization. See FortiGate Session Life Support Protocol (FGSP) on page 1535.

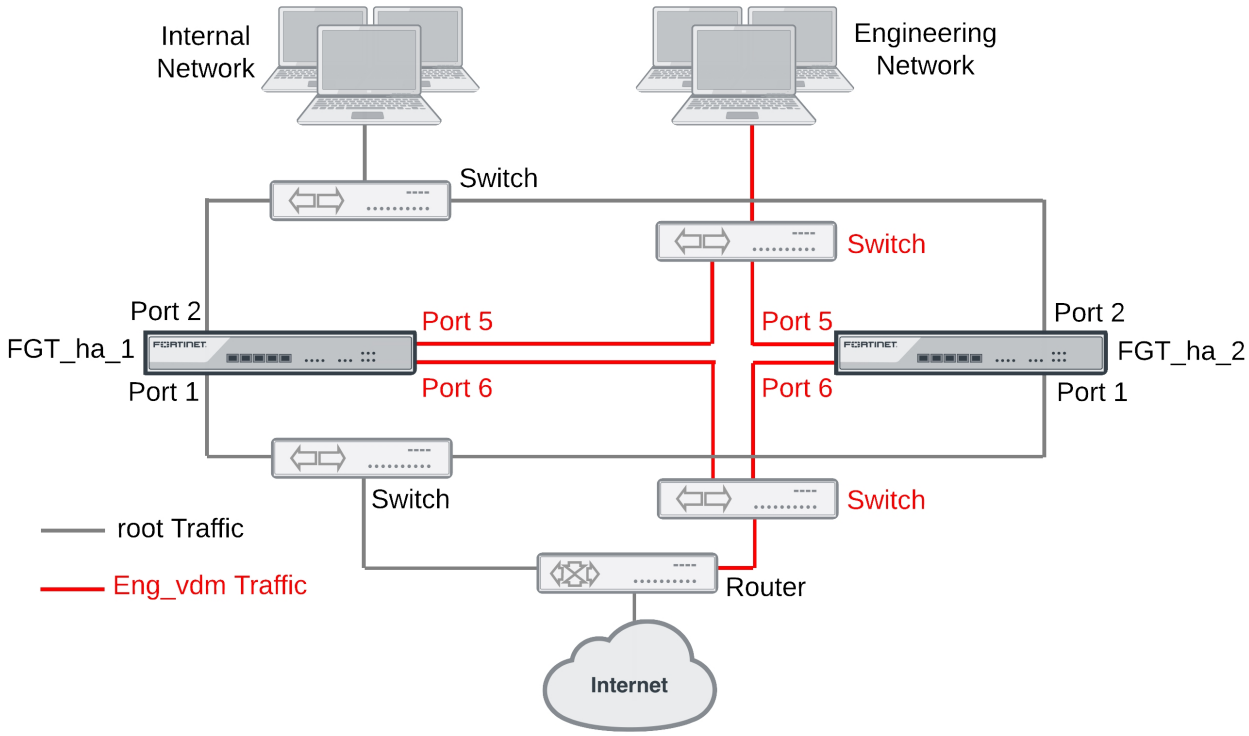
Virtual clustering and failover protection

Virtual clustering operates on a cluster of two (and only two) FortiGate units with VDOMs enabled. Each VDOM creates a cluster between instances of the VDOMs on the two FortiGate units in the virtual cluster. All traffic to and from the VDOM stays within the VDOM and is processed by the VDOM. One cluster unit is the primary unit for each VDOM and one cluster unit is the subordinate unit for each VDOM. The primary unit processes all traffic for the VDOM. The subordinate unit does not process traffic for the VDOM. If a cluster unit fails, all traffic fails over to the cluster unit that is still operating.

Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Example virtual cluster



Virtual clustering and HA override

For a virtual cluster configuration, override is enabled by default for both virtual clusters when you:

- Enable VDOM partionning from the web-based manager by moving virtual domains to virtual cluster 2
- Enter `set vcluster2 enable` from the CLI `config system ha` command to enable virtual cluster 2.

Usually you would enable virtual cluster 2 and expect one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. For this distribution to occur override must be enabled for both virtual clusters. Otherwise you will need to restart the cluster to force it to renegotiate.

If override is enabled the cluster may renegotiate too often.You can choose to disable override at any time. If you decide to disable override, for best results, you should disable it for both cluster units.

For more information about HA override see HA override.

Virtual clustering and load balancing or VDOM partitioning

There are two ways to configure load balancing for virtual clustering. The first is to set the HA mode to active-active. The second is to configure VDOM partitioning. For virtual clustering, setting the HA Mode to active-active has the same result as active-active HA for a cluster without virtual domains. The primary unit receives all

sessions and load balances them among the cluster units according to the load balancing schedule. All cluster units process traffic for all virtual domains.

In a VDOM partitioning virtual clustering configuration, the HA mode is set to active-passive. Even though virtual clustering operates in active-passive mode you can configure a form of load balancing by using VDOM partitioning to distribute traffic between both cluster units. To configure VDOM partitioning you set one cluster unit as the primary unit for some virtual domains and you set the other cluster unit as the primary unit for other virtual domains. All traffic for a virtual domain is processed by the primary unit for that virtual domain. You can control the distribution of traffic between the cluster units by adjusting which cluster unit is the primary unit for each virtual domain.

For example, you could have 4 VDOMs, two of which have a high traffic volume and two of which have a low traffic volume. You can configure each cluster unit to be the primary unit for one of the high volume VDOMs and one of the low volume VDOMs. As a result each cluster unit will be processing traffic for a high volume VDOM and a low volume VDOM, resulting in an even distribution of traffic between the cluster units. You can adjust the distribution at any time. For example, if a low volume VDOM becomes a high volume VDOM you can move it from one cluster unit to another until the best balance is achieved.

From the web-based manager you configure VDOM partitioning by setting the HA mode to active-passive and distributing virtual domains between Virtual Cluster 1 and Virtual Cluster 2. You can also configure different device priorities, port monitoring, and remote link failover, for Virtual Cluster 1 and Virtual Cluster 2.

The device priorities for virtual cluster 1 and virtual cluster 2 are not synchronized between the FortiGate units in the virtual cluster. You must configure these device priorities separately for each cluster unit.

From the CLI you configure VDOM partitioning by setting the HA mode to `a-p`. Then you configure device priority, port monitoring, and remote link failover and specify the VDOMs to include in virtual cluster 1. You do the same for virtual cluster 2 by entering the `config secondary-vcluster` command.

Failover protection does not change. If one cluster unit fails, all sessions are processed by the remaining cluster unit. No traffic interruption occurs for the virtual domains for which the still functioning cluster unit was the primary unit. Traffic may be interrupted temporarily for virtual domains for which the failed unit was the primary unit while processing fails over to the still functioning cluster unit.

If the failed cluster unit restarts and rejoins the virtual cluster, VDOM partitioning load balancing is restored.

Configuring HA for virtual clustering

If your cluster uses VDOMs, you are configuring virtual clustering. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below.

To configure HA options for a cluster with VDOMs enabled:

- Log into the global web-based manager and go to **System > Config > HA**.
- From the CLI, log into the Global Configuration:

The following example shows how to configure active-active virtual clustering:

```
config global
   config system ha
      set mode a-a
      set group-name vexample1.com
```

```
      set password vHA_pass_1
   end
end
```

The following example shows how to configure active-passive virtual clustering:

```
config global
   config system ha
      set mode a-p
      set group-name vexample1.com
      set password vHA_pass_1
   end
end
```

The following example shows how to configure VDOM partitioning for virtual clustering. In the example, the FortiGate unit is configured with three VDOMs (domain_1, domain_2, and domain_3) in addition to the root VDOM. The example shows how to set up a basic HA configuration that sets the device priority of virtual cluster 1 to 200. The example also shows how to enable `vcluster2`, how to set the device priority of virtual cluster 2 to 100 and how to add the virtual domains `domain_2` and `domain_3` to virtual cluster 2.

When you enable multiple VDOMs, `vcluster2` is enabled by default. Even so the command to enable `vcluster2` is included in this example in case for some reason it has been disabled. When `vcluster2` is enabled, `override` is also enabled.

The result of this configuration would be that the cluster unit that you are logged into becomes the primary unit for virtual cluster 1. This cluster unit processes all traffic for the root and domain_1 virtual domains.

```
config global
   config system ha
      set mode a-p
      set group-name vexample1.com
      set password vHA_pass_1
      set priority 200
      set vcluster2 enable
      config secondary-vcluster
         set vdom domain_2 domain_3
         set priority 100
      end
   end
end
```

The following example shows how to use the `execute ha manage` command to change the device priorities for virtual cluster 1 and virtual cluster 2 for the other unit in the cluster. The commands set the device priority of virtual cluster 1 to 100 and virtual cluster 2 to 200.

The result of this configuration would be that the other cluster unit becomes the primary unit for virtual cluster 2. This other cluster unit would process all traffic for the domain_2 and domain_3 virtual domains.

```
config global
   execute ha manage 1
      config system ha
         set priority 100
         set vcluster2 enable
         config secondary-vcluster
            set priority 200
         end
      end
   end
end
```

Example virtual clustering with two VDOMs and VDOM partitioning

This section describes how to configure the example virtual clustering configuration shown below. This configuration includes two virtual domains, root and Eng_vdm and includes VDOM partitioning that sends all root VDOM traffic to FGT_ha_1 and all Eng_vdom VDOM traffic to FGT_ha_2. The traffic from the internal network and the engineering network is distributed between the two FortiGate units in the virtual cluster. If one of the cluster units fails, the remaining unit will process traffic for both VDOMs.

The procedures in this example describe some of many possible sequences of steps for configuring virtual clustering. For simplicity many of these procedures assume that you are starting with new FortiGate units set to the factory default configuration. However, this is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

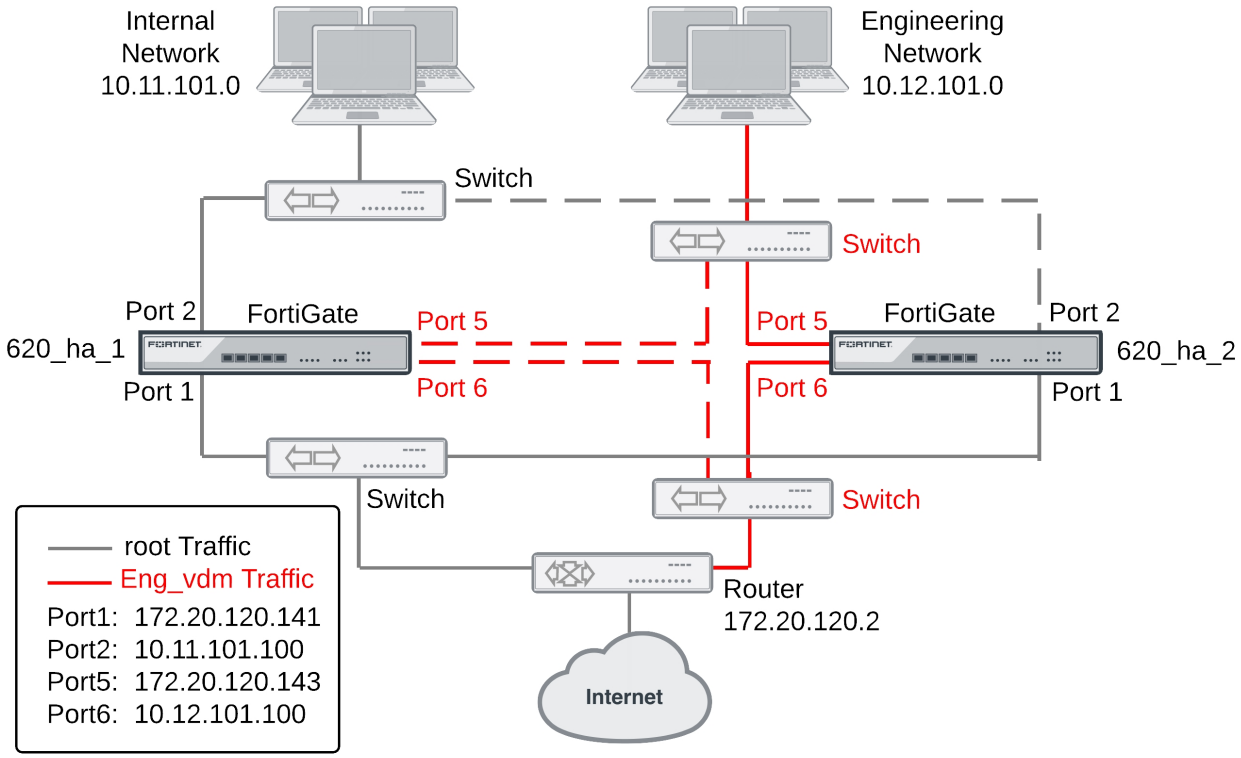
Example virtual clustering network topology

The following figure shows a typical FortiGate HA virtual cluster consisting of two FortiGate units (FGT_ha_1 and FGT_ha_2) connected to and internal network, an engineering network and the Internet. To simplify the diagram the heartbeat connections are not shown.

The traffic from the internal network is processed by the root VDOM, which includes the port1 and port2 interfaces. The traffic from the engineering network is processed by the Eng_vdm VDOM, which includes the port5 and port6 interfaces. VDOM partitioning is configured so that all traffic from the internal network is processed by FGT_ha_1 and all traffic from the engineering network is processed by FGT_ha_2.

This virtual cluster uses the default FortiGate heartbeat interfaces (port3 and port4).

Example virtual cluster showing VDOM partitioning



General configuration steps

The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate units are running the same FortiOS firmware build and are set to the factory default configuration.

General configuration steps

1. Apply licenses to the FortiGate units to become the cluster.
2. Configure the FortiGate units for HA operation.
   - Optionally change each unit's host name.
   - Configure HA.
2. Connect the cluster to the network.
3. Configure VDOM settings for the cluster:
   - Enable multiple VDOMs.
   - Add the Eng_vdm VDOM.
   - Add port5 and port6 to the Eng_vdom.
4. Configure VDOM partitioning.
5. Confirm that the cluster units are operating as a virtual cluster and add basic configuration settings to the cluster.

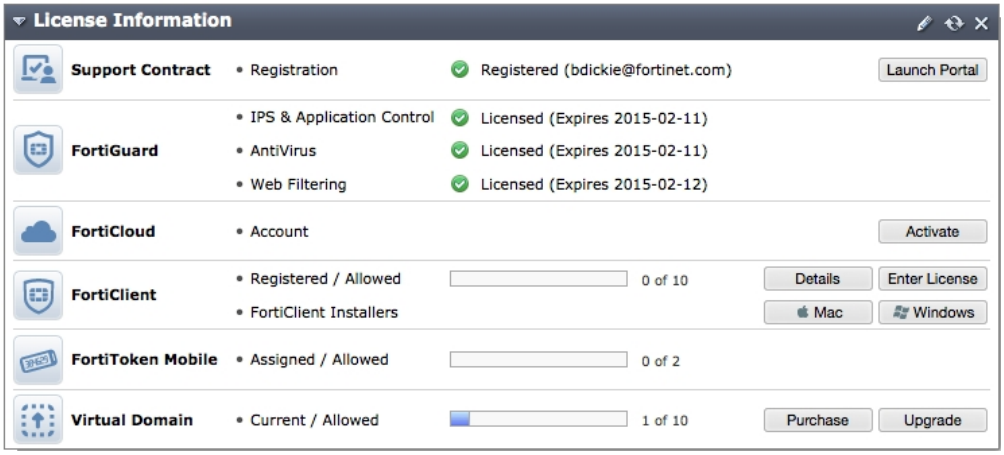
- View cluster status from the web-based manager or CLI.
- Add a password for the admin administrative account.
- Change the IP addresses and netmasks of the port1, port2, port5, and port6 interfaces.
- Add a default routes to each VDOM.

Configuring virtual clustering with two VDOMs and VDOM partitioning - web-based manager

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Select **OK**.
6. Go to **System > Config > HA** and change the following settings.

Mode	Active-Passive
Group Name	vexample2.com
Password	vHA_pass_2

7. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces (see Cluster virtual MAC addresses). The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

7. Power off the first FortiGate unit.
8. Repeat these steps for the second FortiGate unit.
   Set the second FortiGate unit host name to:

New Name	FGT_ha_2

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 to switch connected to the Internet.
   You could use the same switch for the port1 and port5 interfaces.
3. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
4. Connect the port6 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the engineering network.
5. Connect the port3 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
6. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
7. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.

   When negotiation is complete you can continue.

To configure VDOM settings for the cluster

1. Log into the web-based manager.
2. On the **System Information** dashboard widget, beside **Virtual Domain** select **Enable**.
3. Select **OK** and then log back into the web-based manager.
4. Go to **System > VDOM** and select **Create New** to add a new VDOM.

Name	Eng_vdm

5. Go to **System > Network > Interfaces**.
6. Edit the **port5** interface, add it to the Eng_vdm VDOM and configure other interface settings:

Alias	Engineering_external
Virtual Domain	Eng_vdm
IP/Netmask	172.20.120.143/24

7. Select **OK**.
8. Edit the **port6** interface, add it to the Eng_vdm VDOM and configure other interface settings:

Alias	Engineering_internal
Virtual Domain	Eng_vdm
IP/Netmask	10.120.101.100/24
Administrative Access	HTTPS, PING, SSH

9. Select **OK**.

To add a default route to each VDOM

1. Go to **System > VDOM** and Enter the root VDOM.
2. Go to **Router > Static > Static Routes**.
3. Change the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	port1
Distance	10

4. Select **Global**.
5. Go to **System > VDOM** and Enter the Eng_vdm VDOM.
6. Go to **Router > Static > Static Routes**.
7. Change the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	port5
Distance	10

To configure VDOM partitioning

1. Go to **System > Config > HA**.
   The cluster members shows two cluster units in Virtual Cluster 1.
2. Edit the cluster unit with the **Role** of **MASTER**.
3. Change **VDOM partitioning** to move the **Eng_vdm** to the **Virtual Cluster 2** list.
4. Select **OK**.
5. Change the Virtual Cluster 1 and Virtual Cluster 2 device priorities for each cluster unit to the following:

	Device Priority	
Host Name	**Virtual Cluster 1**	**Virtual Cluster 2**
FGT_ha_1	200	100
FGT_ha_2	100	200

You can do this by editing the HA configurations of each cluster unit in the cluster members list and changing device priorities.

Since the device priority of Virtual Cluster 1 is highest for FGT_ha_1 and since the root VDOM is in Virtual Cluster 1, all traffic for the root VDOM is processed by FGT_ha_1.

Since the device priority of Virtual Cluster 2 is highest for FGT_ha_2 and since the Eng_vdm VDOM is in Virtual Cluster 2, all traffic for the Eng_vdm VDOM is processed by FGT_ha_2.

To view cluster status and verify the VDOM partitioning configuration

1. Log into the web-based manager.
2. Go to **System > Config > HA**.
   The cluster members list should show the following:
   - Virtual Cluster 1 contains the root VDOM.
   - FGT_ha_1 is the primary unit (master) for Virtual Cluster 1.
   - Virtual Cluster 2 contains the Eng_vdm VDOM.
   - FGT_ha_2 is the primary unit (master) for Virtual Cluster 2.

To test the VDOM partitioning configuration

You can do the following to confirm that traffic for the root VDOM is processed by FGT_ha_1 and traffic for the Eng_vdm is processed by FGT_ha_2.

1. Log into the web-based manager by connecting to port2 using IP address 10.11.101.100.
   You will log into FGT_ha_1 because port2 is in the root VDOM and all traffic for this VDOM is processed by FGT_ha_1. You can confirm that you have logged into FGT_ha_1 by checking the host name on the System Information dashboard widget.
2. Log into the web-based manager by connecting to port6 using IP address 10.12.101.100.
   You will log into FGT_ha_2 because port6 is in the Eng_vdm VDOM and all traffic for this VDOM is processed by FGT_ha_2.
3. Add security policies to the root virtual domain that allows communication from the internal network to the Internet and connect to the Internet from the internal network.
4. Log into the web-based manager and go to **Config > System > HA** and select **View HA Statistics**.
   The statistics display shows more active sessions, total packets, network utilization, and total bytes for the FGT_ha_1 unit.
5. Add security policies to the Eng_vdm virtual domain that allow communication from the engineering network to the Internet and connect to the Internet from the engineering network.
6. Log into the web-based manager and go to **Config > System > HA** and select **View HA Statistics**.
   The statistics display shows more active sessions, total packets, network utilization, and total bytes for the FGT_ha_2 unit.

Configuring virtual clustering with two VDOMs and VDOM partitioning - CLI

These procedures assume you are starting with two FortiGate units with factory default settings.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.

FortiToken licenses can be added at any time because they are synchronized to all cluster members.

3. Change the host name for this FortiGate unit:

```
config system global
   set hostname FGT_ha_1
end
```

4. Configure HA settings.

```
config system ha
   set mode a-p
   set group-name vexample2.com
   set password vHA_pass_2
end
```

The FortiGate unit negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces (see Cluster virtual MAC addresses). The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
```

```
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

4. Power off the first FortiGate unit.
5. Repeat these steps for the second FortiGate unit.
   Set the other FortiGate unit host name to:

```
config system global
   set hostname FGT_ha_2
end
```

To connect the cluster to the network

1. Connect the port1 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the Internet.
2. Connect the port5 interfaces of FGT_ha_1 and FGT_ha_2 to switch connected to the Internet.
   You could use the same switch for port1 and port5.
3. Connect the port2 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the internal network.
4. Connect the port6 interfaces of FGT_ha_1 and FGT_ha_2 to a switch connected to the engineering network.
5. Connect the port3 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
6. Connect the port4 interfaces of the cluster units together. You can use a crossover Ethernet cable or regular Ethernet cables and a switch.
7. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.

   When negotiation is complete you can continue.

To configure VDOM settings for the cluster

1. Log into the CLI.
2. Enter the following command to enable multiple VDOMs for the cluster.

```
config system global
   set vdom-admin enable
end
```

3. Log back into the CLI.
4. Enter the following command to add the Eng_vdm VDOM:

```
config vdom
   edit Eng_vdm
end
```

5. Edit the port5 interface, add it to the Eng_vdm VDOM and configure other interface settings:

```
config global
   config system interface
      edit port5
         set vdom Eng_vdm
```

```
        set alias Engineering_external
        set ip 172.20.12.143/24
      next
      edit port6
        set vdom Eng_vdm
        set alias Engineering_internal
        set ip 10.120.101.100/24
      end
end
```

To add a default route to each VDOM

1. Enter the following command to add default routes to the root and Eng_vdm VDOMs.

```
config vdom
  edit root
    config router static
      edit 1
        set dst 0.0.0.0/0.0.0.0
        set gateway 172.20.120.2
        set device port1
      end
  next
  edit Eng_vdm
    config router static
      edit 1
        set dst 0.0.0.0/0.0.0.0
        set gateway 172.20.120.2
        set device port5
      end
end
```

To configure VDOM partitioning

1. Enter the `get system ha status` command to view cluster unit status:
   For example, from the FGT_ha_2 cluster unit CLI:

```
config global
  get system ha status
    Model: XXXX
    Mode: a-p
    Group: 0
    Debug: 0
    ses_pickup: disable
    Master:128 FGT_ha_2 FG600B3908600825 0
    Slave :128 FGT_ha_1 FG600B3908600705 1
    number of vcluster: 1
    vcluster 1: work 169.254.0.1
    Master:0 FG600B3908600825
    Slave :1 FG600B3908600705
```

   This command output shows that VDOM partitioning has not been configured because only virtual cluster 1 is shown. The command output also shows that the FGT_ha_2 is the primary unit for the cluster and for virtual cluster 1 because this cluster unit has the highest serial number

2. Enter the following commands to configure VDOM partitioning:

```
config global
  config system ha
```

```
        set vcluster2 enable
           config secondary-vcluster
              set vdom Eng_vdm
           end
     end
end
```

3. Enter the `get system ha status` command to view cluster unit status:
   For example, from the FGT_ha_2 cluster unit CLI:

```
config global
   get system ha status
      Model: XXXX
      Mode: a-p
      Group: 0
      Debug: 0
      ses_pickup: disable
      Master:128 FGT_ha_2 FG600B3908600825 0
      Slave :128 FGT_ha_1 FG600B3908600705 1
      number of vcluster: 2
      vcluster 1: work 169.254.0.1
      Master:0 FG600B3908600825
      Slave :1 FG600B3908600705
      vcluster 2: work 169.254.0.1
      Master:0 FG600B3908600825
      Slave :1 FG600B3908600705
```

   This command output shows VDOM partitioning has been configured because both virtual cluster 1 and virtual cluster 2 are visible. However the configuration is not complete because FGT_ha_2 is the primary unit for both virtual clusters. The command output shows this because under both vcluster entries the `Master` entry shows `FG600B3908600825`, which is the serial number of FGT_ha_2. As a result of this configuration, FGT_ha_2 processes traffic for both VDOMs and FGT_ha_1 does not process any traffic.

4. Change the Virtual Cluster 1 and Virtual Cluster 2 device priorities for each cluster unit so that FGT_ha_1 processes virtual cluster 1 traffic and FGT_ha_2 processes virtual cluster 2 traffic.
   Since the root VDOM is in virtual cluster 1 and the Eng_vdm VDOM is in virtual cluster 2 the result of this configuration will be that FGT_ha_1 will process all root VDOM traffic and FGT_ha_2 will process all Eng_vdm traffic. You make this happen by changing the cluster unit device priorities for each virtual cluster. You could use the following settings:

		Device Priority
Host Name	**Virtual Cluster 1**	**Virtual Cluster 2**
FGT_ha_1	200	100
FGT_ha_2	100	200

   Since the device priority is not synchronized you can edit the device priorities of each virtual cluster on each FortiGate unit separately. To do this:

   - Log into the CLI and note the FortiGate unit you have actually logged into (for example, by checking the host name displayed in the CLI prompt).
   - Change the virtual cluster 1 and 2 device priorities for this cluster unit.

- Then use the `execute ha manage` command to log into the other cluster unit CLI and set its virtual cluster 1 and 2 device priorities.

Enter the following commands from the FGT_ha_1 cluster unit CLI:

```
config global
   config system ha
      set priority 200
         config secondary-vcluster
            set priority 100
         end
   end
end
```

Enter the following commands from the FGT_ha_2 cluster unit CLI:

```
config global
   config system ha
      set priority 100
         config secondary-vcluster
            set priority 200
         end
   end
end
```

The cluster may renegotiate during this step resulting in a temporary loss of connection to the CLI and a temporary service interruption.

Since the device priority of Virtual Cluster 1 is highest for FGT_ha_1 and since the root VDOM is in Virtual Cluster 1, all traffic for the root VDOM is processed by FGT_ha_1.

Since the device priority of Virtual Cluster 2 is highest for FGT_ha_2 and since the Eng_vdm VDOM is in Virtual Cluster 2, all traffic for the Eng_vdm VDOM is processed by FGT_ha_2.

To verify the VDOM partitioning configuration

1. Log into the FGT_ha_2 cluster unit CLI and enter the following command:

```
config global
   get system ha status
      Model: XXXX
      Mode: a-p
      Group: 0
      Debug: 0
      ses_pickup: disable
      Slave :100 FGT_ha_2 FG600B3908600825 0
      Master:200 FGT_ha_1 FG600B3908600705 1
      number of vcluster: 2
      vcluster 1: standby 169.254.0.2
      Slave :1 FG600B3908600825
      Master:0 FG600B3908600705
      vcluster 2: work 169.254.0.1
      Master:0 FG600B3908600825
      Slave :1 FG600B3908600705
```

The command output shows that FGT_ha_1 is the primary unit for virtual cluster 1 (because the command output show the `Master` of virtual cluster 1 is the serial number of FGT_ha_1) and that

FGT_ha_2 is the primary unit for virtual cluster 2.

If you enter the same command from the FGT_ha_1 CLI the same information is displayed but in a different order. The command always displays the status of the cluster unit that you are logged into first.

```
config global
   get system ha status
      Model: XXXX
      Mode: a-p
      Group: 0
      Debug: 0
      ses_pickup: disable
      Master:200 FGT_ha_1 FG600B3908600705 1
      Slave :100 FGT_ha_2 FG600B3908600825 0
      number of vcluster: 2
      vcluster 1: work 169.254.0.2
      Master:0 FG600B3908600705
      Slave :1 FG600B3908600825
      vcluster 2: standby 169.254.0.1
      Slave :1 FG600B3908600705
      Master:0 FG600B3908600825
```

To test the VDOM partitioning configuration

You can do the following to confirm that traffic for the root VDOM is processed by FGT_ha_1 and traffic for the Eng_vdm is processed by FGT_ha_2. These steps assume the cluster is operating correctly.

1. Log into the CLI by connecting to port2 using IP address 10.11.101.100.
   You will log into FGT_ha_1 because port2 is in the root VDOM and all traffic for this VDOM is processed by FGT_ha_1. You can confirm that you have logged into FGT_ha_1 by checking the host name in the CLI prompt. Also the `get system status` command displays the status of the FGT_ha_1 cluster unit.
2. Log into the web-based manager or CLI by connecting to port6 using IP address 10.12.101.100.
   You will log into FGT_ha_2 because port6 is in the Eng_vdm VDOM and all traffic for this VDOM is processed by FGT_ha_2.
3. Add security policies to the root virtual domain that allow communication from the internal network to the Internet and connect to the Internet from the internal network.
4. Log into the web-based manager and go to **Config > System > HA** and select **View HA Statistics**.
   The statistics display shows more active sessions, total packets, network utilization, and total bytes for the FGT_ha_1 unit.
5. Add security policies to the Eng_vdm virtual domain that allow communication from the engineering network to the Internet and connect to the Internet from the engineering network.
6. Log into the web-based manager and go to **Config > System > HA** and select **View HA Statistics**.
   The statistics display shows more active sessions, total packets, network utilization, and total bytes for the FGT_ha_2 unit.

Example inter-VDOM links in a virtual clustering configuration

In a virtual domain configuration you can use inter-VDOM links to route traffic between two virtual domains operating in a single FortiGate unit without using physical interfaces. Adding an inter-VDOM link has the affect of adding two interfaces to the FortiGate unit and routing traffic between the virtual domains using the inter-VDOM link interfaces.

In a virtual clustering configuration inter-VDOM links can only be made between virtual domains that are in the same virtual cluster. So, if you are planning on configuring inter-VDOM links in a virtual clustering configuration, you should make sure the virtual domains that you want to link are in the same virtual cluster.

For example, the following tables show an example virtual clustering configuration where each virtual cluster contains four virtual domains. In this configuration you can configure inter-VDOM links between root and vdom_1 and between vdom_2 and vdom_3. But, you cannot configure inter-VDOM links between root and vdom_2 or between vdom_1 and vdom_3 (and so on).

		Hostname
Virtual Domains	**FortiGate_A**	**FortiGate_B**
root	**Priority**	**Priority**
	200	100
vdom_1	**Role**	**Role**
	Primary	Subordinate

		Hostname
Virtual Domains	**FortiGate_A**	**FortiGate_B**
vdom_2	**Priority**	**Priority**
	100	200
vdom_3	**Role**	**Role**
	Subordinate	Primary

Configuring inter-VDOM links in a virtual clustering configuration

Configuring inter-VDOM links in a virtual clustering configuration is very similar to configuring inter-VDOM links for a standalone FortiGate unit. The main difference the `config system vdom-link` command includes the `vcluster` keyword. The default setting for `vcluster` is `vcluster1`. So you only have to use the `vcluster` keyword if you are added an inter-VDOM link to virtual cluster 2.

To add an inter-VDOM link to virtual cluster 1

This procedure describes how to create an inter-VDOM link to virtual cluster 1 that results in a link between the root and vdom_1 virtual domains.

Inter-VDOM links are also called internal point-to-point interfaces.

1. Add an inter-VDOM link called `vc1link`.

```
config global
   config system vdom-link
   edit vc1link
end
```

   Adding the inter-VDOM link also adds two interfaces. In this example, these interfaces are called `vc1link0` and `vc1link1`. These interfaces appear in all CLI and web-based manager interface lists. These interfaces can only be added to virtual domains in virtual cluster 1.

2. Bind the `vc1link0` interface to the root virtual domain and bind the `vc1link1` interface to the vdom_1 virtual domain.

```
config system interface
   edit vc1link0
        set vdom root
   next
   edit vc1link1
      set vdom vdom_1
   end
```

To add an inter-VDOM link to virtual cluster 2

This procedure describes how to create an inter-VDOM link to virtual cluster 2 that results in a link between the vdom_2 and vdom_3 virtual domains.

1. Add an inter-VDOM link called `vc2link`.

```
config global
   config system vdom-link
      edit vc2link
         set vcluster vcluster2
      end
```

   Adding the inter-VDOM link also adds two interfaces. In this example, these interfaces are called `vc2link0` and `vc2link1`. These interfaces appear in all CLI and web-based manager interface lists. These interfaces can only be added to virtual domains in virtual cluster 2.

2. Bind the `vc2link0` interface to the vdom_2 virtual domain and bind the `vc2link1` interface to the vdom_3 virtual domain.

```
config system interface
   edit vc2link0
      set vdom vdom_2
   next
   edit vc2link1
      set vdom vdom_3
   end
```

Troubleshooting virtual clustering

Troubleshooting virtual clusters is similar to troubleshooting any cluster (see FGCP configuration examples and troubleshooting on page 1313). This section describes a few testing and troubleshooting techniques for virtual clustering.

To test the VDOM partitioning configuration

You can do the following to confirm that traffic for different VDOMs will be distributed among both FortiGate units in the virtual cluster. These steps assume the cluster is otherwise operating correctly.

1. Log into the web-based manager or CLI using the IP addresses of interfaces in each VDOM.
   Confirm that you have logged into the FortiGate unit that should be processing traffic for that VDOM by checking the HTML title displayed by your web browser or the CLI prompt. Both of these should include the host name of the cluster unit that you have logged into. Also on the system Dashboard, the System Information widget displays the serial number of the FortiGate unit that you logged into. From the CLI the `get system status` command displays the status of the cluster unit that you logged into.
2. To verify that the correct cluster unit is processing traffic for a VDOM:
   - Add security policies to the VDOM that allow communication between the interfaces in the VDOM.
   - Optionally enable traffic logging and other monitoring for that VDOM and these security policies.
   - Start communication sessions that pass traffic through the VDOM.
   - Log into the web-based manager and go to **Config > System > HA** and select **View HA Statistics**. Verify that the statistics display shows more active sessions, total packets, network utilization, and total bytes for the unit that should be processing all traffic for the VDOM.
   - Optionally check traffic logging and the Top Sessions Widget for the FortiGate unit that should be processing traffic for that VDOM to verify that the traffic is being processed by this FortiGate unit.

Full mesh HA

This chapter provides an introduction to full mesh HA and also contains general procedures and configuration examples that describe how to configure FortiGate full mesh HA.

The examples in this chapter include example values only. In most cases you will substitute your own values. The examples in this chapter also do not contain detailed descriptions of configuration parameters.

Full mesh HA overview

When two or more FortiGate units are connected to a network in an HA cluster the reliability of the network is improved because the HA cluster replaces a single FortiGate unit as a single point of failure. With a cluster, a single FortiGate unit is replaced by a cluster of two or more FortiGate units.

However, even with a cluster, potential single points of failure remain. The interfaces of each cluster unit connect to a single switch and that switch provides a single connection to the network. If the switch fails or if the connection between the switch and the network fails service is interrupted to that network.

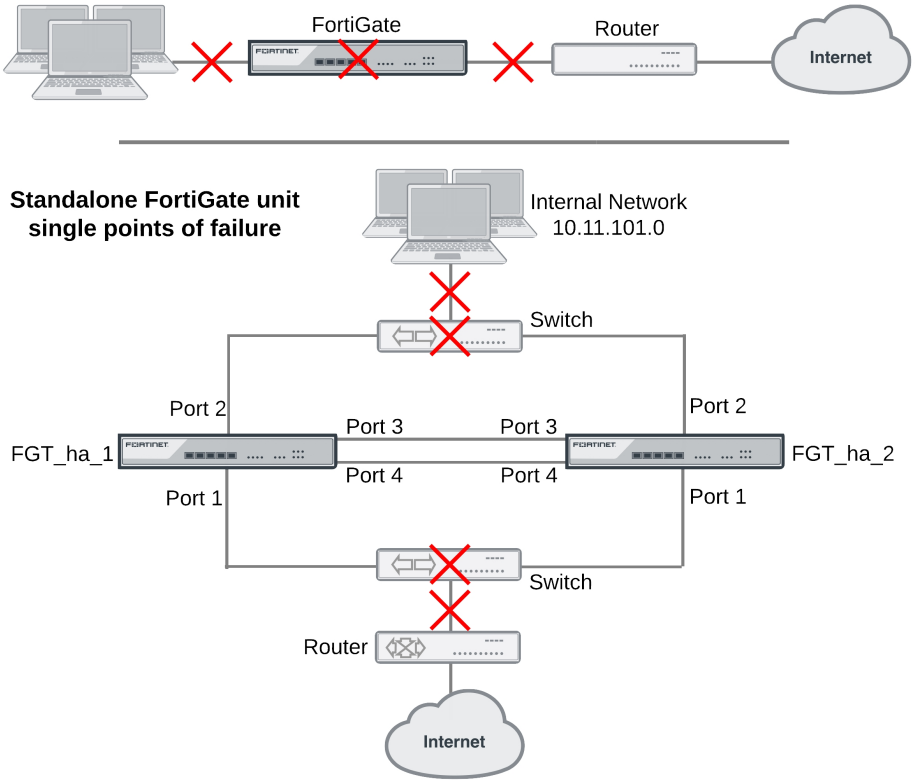
The HA cluster does improve the reliability of the network because switches are not as complex components as FortiGate units, so are less likely to fail. However, for even greater reliability, a configuration is required that includes redundant connections between the cluster the networks that it is connected to.

FortiGate models that support 802.3ad Aggregate or Redundant interfaces can be used to create a cluster configuration called full mesh HA. Full mesh HA is a method of reducing the number of single points of failure on a network that includes an HA cluster.

This redundant configuration can be achieved using FortiGate 802.3ad Aggregate or Redundant interfaces and a full mesh HA configuration. In a full mesh HA configuration, you connect an HA cluster consisting of two or more FortiGate units to the network using 802.3ad Aggregate or Redundant interfaces and redundant switches. Each 802.3ad Aggregate or Redundant interface is connected to two switches and both of these switches are connected to the network. In addition you must set up an IEEE 802.1Q (also called Dot1Q) or ISL link between the redundant switches connected to the Aggregate or Redundant interfaces.

The resulting full mesh configuration, an example is shown below, includes redundant connections between all network components. If any single component or any single connection fails, traffic automatically switches to the redundant component and connection and traffic flow resumes.

Single points of failure in a standalone and HA network configuration



Full mesh HA and redundant heartbeat interfaces

A full mesh HA configuration also includes redundant HA heartbeat interfaces. At least two heartbeat interfaces should be selected in the HA configuration and both sets of HA heartbeat interfaces should be connected. The HA heartbeat interfaces do not have to be configured as redundant interfaces because the FGCP handles failover between heartbeat interfaces.

Full mesh HA, redundant interfaces and 802.3ad aggregate interfaces

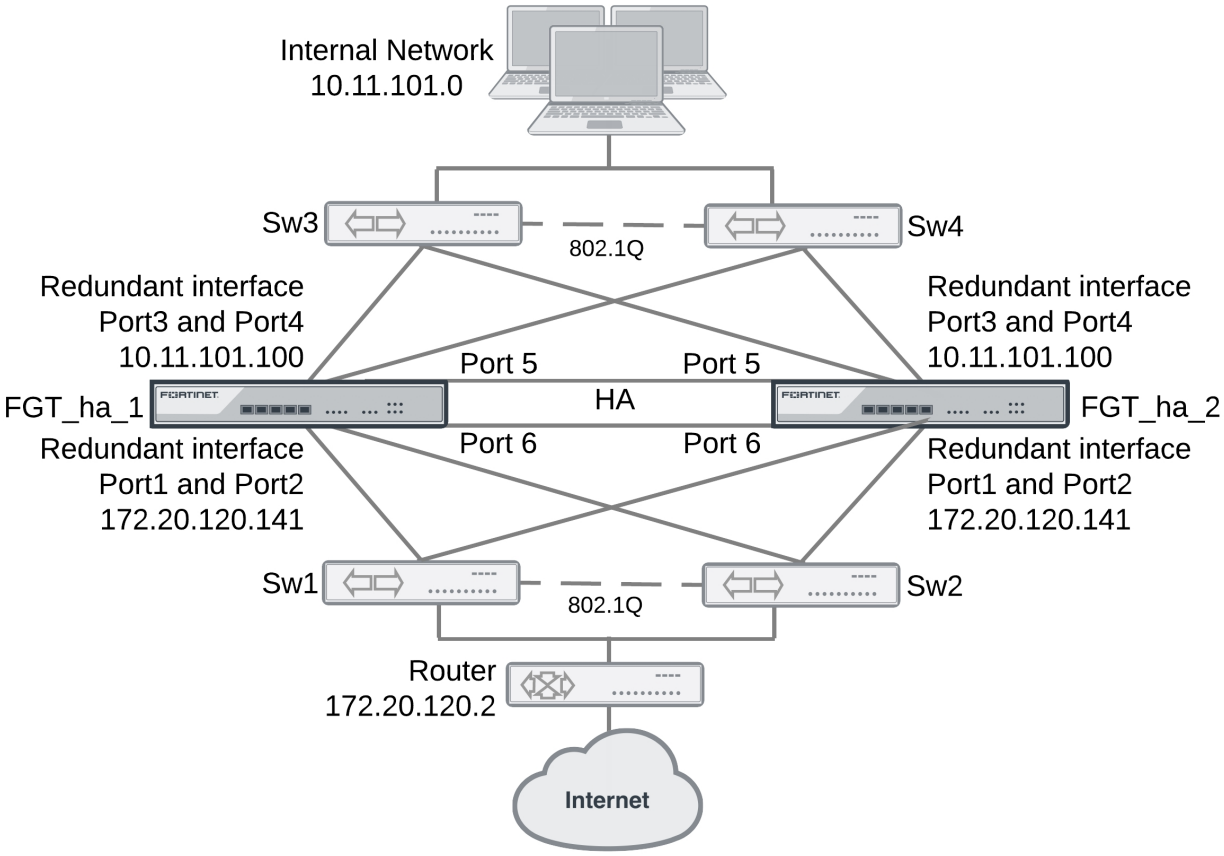
Full mesh HA is supported for both redundant interfaces and 802.3ad aggregate interfaces. In most cases you would simply use redundant interfaces. However, if your switches support 802.3ad aggregate interfaces and split multi-trunking you can use aggregate interfaces in place of redundant interfaces for full mesh HA. One advantage of using aggregate interfaces is that all of the physical interfaces in the aggregate interface can send and receive packets. As a result, using aggregate interfaces may increase the bandwidth capacity of the cluster.

Usually redundant and aggregate interfaces consist of two physical interfaces. However, you can add more than two physical interfaces to a redundant or aggregate interface. Adding more interfaces can increase redundancy protection. Adding more interfaces can also increase bandwidth capacity if you are using 802.3ad aggregate interfaces.

Example full mesh HA configuration

The following figure shows a full mesh HA configuration with a cluster of two FortiGate units. This section describes the FortiGate configuration settings and network components required for a full mesh HA configuration. This section also contains example steps for setting up this full mesh HA configuration. The procedures in this section describe one of many possible sequences of steps for configuring full mesh HA. As you become more experienced with FortiOS, HA, and full mesh HA you may choose to use a different sequence of configuration steps.

Full Mesh HA configuration



For simplicity these procedures assume that you are starting with two new FortiGate units set to the factory default configuration. However, starting from the default configuration is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

These procedures describe how to configure a cluster operating in NAT/Route mode because NAT/Route is the default FortiGate operating mode. However, the steps are the same if the cluster operates in Transparent mode. You can either switch the cluster units to operate in Transparent mode before beginning these procedures, or you can switch the cluster to operate in Transparent mode after HA is configured and the cluster is connected and operating.

Full mesh HA configuration

The two FortiGate units (FGT_ha_1 and FGT_ha_2) can be operating in NAT/Route or Transparent mode. Aside from the standard HA settings, the FortiGate configuration includes the following:

- The port5 and port6 interfaces configured as heartbeat interfaces. A full mesh HA configuration also includes redundant HA heartbeat interfaces.
- The port1 and port2 interfaces added to a redundant interface. Port1 is the active physical interface in this redundant interface. To make the port1 interface the active physical interface it should appear above the port2 interface in the redundant interface configuration.
- The port3 and port4 interfaces added to a redundant interface. Port3 is the active physical interface in this redundant interface. To make the port3 interface the active physical interface it should appear above the port4 interface in the redundant interface configuration.

Full mesh switch configuration

The following redundant switch configuration is required:

- Two redundant switches (Sw3 and Sw4) connected to the internal network. Establish an 802.1Q (Dot1Q) or interswitch-link (ISL) connection between them.
- Two redundant switches (Sw1 and Sw2) connected to the Internet. Establish an 802.1Q (Dot1Q) or interswitch-link (ISL) connection between them.

Full mesh network connections

Make the following physical network connections for FGT_ha_1:

- Port1 to Sw1 (active)
- Port2 to Sw2 (inactive)
- Port3 to Sw3 (active)
- Port4 to Sw4 (inactive)

Make the following physical network connections for FGT_ha_2:

- Port1 to Sw2 (active)
- Port2 to Sw1 (inactive)
- Port3 to Sw4 (active)
- Port4 to Sw3 (inactive)

How packets travel from the internal network through the full mesh cluster and to the Internet

If the cluster is operating in active-passive mode and FGT_ha_2 is the primary unit, all packets take the following path from the internal network to the internet:

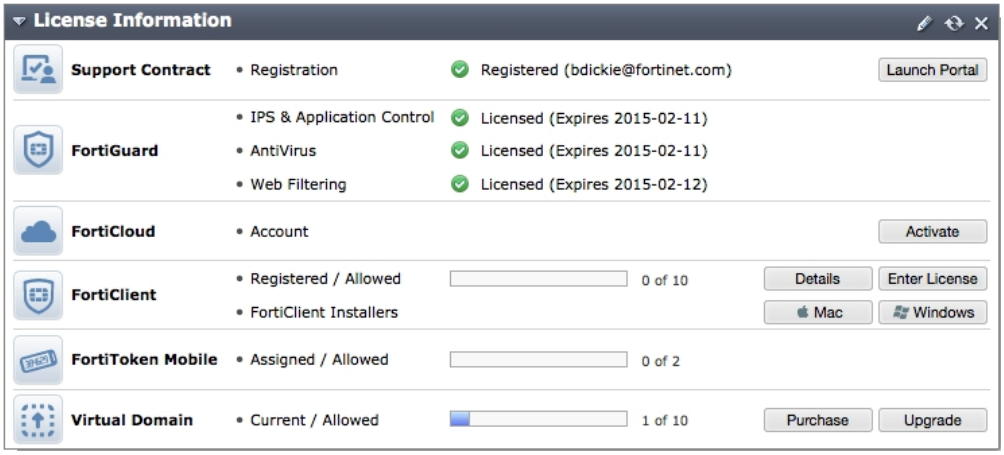
1. From the internal network to Sw4. Sw4 is the active connection to FGT_ha_2; which is the primary unit. The primary unit receives all packets.
2. From Sw4 to the FGT_ha_2 port3 interface. Active connection between Sw4 and FGT_ha_2. Port3 is the active member of the redundant interface.
3. From FGT_ha_2 port3 to FGT_ha_2 port1. Active connection between FGT_ha_2 and Sw2. Port1 is the active member of the redundant interface.
4. From Sw2 to the external router and the Internet.

Configuring full-mesh HA - web-based manager

Each cluster unit must have the same HA configuration.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation, and **FortiClient** licensing licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).



2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. On the **System Information** dashboard widget, beside **Host Name** select **Change**.
4. Enter a new Host Name for this FortiGate unit.

New Name	FGT_ha_1

5. Go to **System > Config > HA** and change the following settings.

Mode	Active-Active	
Group Name	Rexample1.com	
Password	RHA_pass_1	
Heartbeat Interface		
	Enable	**Priority**
port5	Select	50
port6	Select	50

6. Select **OK**.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to

the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

6. Power off the first FortiGate unit.
7. Repeat these steps for the second FortiGate unit.
   Set the second FortiGate unit host name to:

New Name	FGT_ha_2

To connect the cluster to your network

1. Make the following physical network connections for FGT_ha_1:
   - Port1 to Sw1 (active)
   - Port2 to Sw2 (inactive)
   - Port3 to Sw3 (active)
   - Port4 to Sw4 (inactive)
2. Make the following physical network connections for FGT_ha_2:
   - Port1 to Sw2 (active)
   - Port2 to Sw1 (inactive)
   - Port3 to Sw4 (active)
   - Port4 to Sw3 (inactive)
3. Connect Sw3 and Sw4 to the internal network.
4. Connect Sw1 and Sw2 to the external router.
5. Enable 802.1Q (Dot1Q) or ISL communication between Sw1 and Sw2 and between Sw3 and Sw4.
6. Power on the cluster units.

   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster.

1. View the system dashboard.

   The System Information dashboard widget shows the **Cluster Name** (Rexample1.com) and the host names and serial numbers of the **Cluster Members**. The Unit Operation widget shows multiple cluster units.
2. Go to **System > Config > HA** to view the cluster members list.

   The list shows two cluster units, their host names, their roles in the cluster, and their priorities. You can use this list to confirm that the cluster is operating normally.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard does not display information for both cluster units the FortiGate units are not functioning as a cluster. See Troubleshooting full mesh HA on page 1419 to troubleshoot the cluster.

To add basic configuration settings and the redundant interfaces

Use the following steps to add a few basic configuration settings.

1. Log into the cluster web-based manager.
2. Go to **System > Admin > Administrators**.
3. Edit **admin** and select **Change Password**.
4. Enter and confirm a new password.

5. Select **OK**.
6. Go to **Router > Static > Static Routes** and temporarily delete the default route.
   You cannot add an interface to a redundant interface if any settings (such as the default route) are configured for it.
7. Go to **System > Network > Interfaces** and select **Create New** and configure the redundant interface to connect to the Internet.

Name	Port1_Port2
Type	Redundant
Physical Interface Members	
Selected Interfaces	port1, port2
IP/Netmask	172.20.120.141/24

8. Select **OK**.
9. Select **Create New** and configure the redundant interface to connect to the internal network.

Name	Port3_Port4
Type	Redundant
Physical Interface Members	
Selected Interfaces	port3, port4
IP/Netmask	10.11.101.100/24
Administrative Access	HTTPS, PING, SSH

10. Select **OK**.
    The virtual MAC addresses of the FortiGate interfaces change to the following. Notice that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:
    - port1 interface virtual MAC: `00-09-0f-09-00-00`
    - port10 interface virtual MAC: `00-09-0f-09-00-01`
    - port11 interface virtual MAC: `00-09-0f-09-00-02`
    - port12 interface virtual MAC: `00-09-0f-09-00-03`
    - port13 interface virtual MAC: `00-09-0f-09-00-04`
    - port14 interface virtual MAC: `00-09-0f-09-00-05`
    - port15 interface virtual MAC: `00-09-0f-09-00-06`
    - port16 interface virtual MAC: `00-09-0f-09-00-07`
    - port17 interface virtual MAC: `00-09-0f-09-00-08`
    - port18 interface virtual MAC: `00-09-0f-09-00-09`
    - port19 interface virtual MAC: `00-09-0f-09-00-0a`
    - port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)

- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

11. Go to **Router > Static > Static Routes**.
12. Add the default route.

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	172.20.120.2
Device	Port1_Port2
Distance	10

13. Select **OK**.

To configure HA port monitoring for the redundant interfaces

1. Go to **System > Config > HA**.
2. In the cluster members list, edit the primary unit.
3. Configure the following port monitoring for the redundant interfaces:

	Port Monitor
Port1_Port2	Select
Port3_Port4	Select

4. Select **OK**.

Configuring Full Mesh HA - CLI

Each cluster must have the same HA configuration. Use the following procedure to configure the FortiGate units for HA operation.

To configure the FortiGate units for HA operation

1. Register and apply licenses to the FortiGate unit. This includes **FortiCloud** activation, and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMS).
2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.
   FortiToken licenses can be added at any time because they are synchronized to all cluster members.
3. Enter a new Host Name for this FortiGate unit.

```
config system global
   set hostname FGT_ha_1
```

```
end
```

4. Configure HA settings.

```
config system ha
   set mode a-a
   set group-name Rexample1.com
   set password RHA_pass_1
   set hbdev port5 50 port6 50
end
```

The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and the FGCP changes the MAC address of the FortiGate unit interfaces. The MAC addresses of the FortiGate interfaces change to the following virtual MAC addresses:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-0b`
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0e`
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

You can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) CLI command to view the virtual MAC address of any FortiGate unit interface. For example, use the following command to view the port1 interface virtual MAC address (`Current_HWaddr`) and the port1 permanent MAC address (`Permanent_HWaddr`):

```
get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:00
```

```
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

4. Power off the first FortiGate unit.
5. Repeat these steps for the second FortiGate unit.
   Set the other FortiGate unit host name to:

```
config system global
   set hostname FGT_ha_2
end
```

To connect the cluster to your network

1. Make the following physical network connections for FGT_ha_1:
   - Port1 to Sw1 (active)
   - Port2 to Sw2 (inactive)
   - Port3 to Sw3 (active)
   - Port4 to Sw4 (inactive)
2. Make the following physical network connections for FGT_ha_2:
   - Port1 to Sw2 (active)
   - Port2 to Sw1 (inactive)
   - Port3 to Sw4 (active)
   - Port4 to Sw3 (inactive)
3. Connect Sw3 and Sw4 to the internal network.
4. Connect Sw1 and Sw2 to the external router.
5. Enable 802.1Q (Dot1Q) or ISL communication between Sw1 and Sw2 and between Sw3 and Sw4.
6. Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.

   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status

Use the following steps to view cluster status from the CLI.

1. Log into the CLI.
2. Enter `get system status` to verify the HA status of the cluster unit that you logged into.
   If the command output includes `Current HA mode: a-a, master`, the cluster units are operating as a cluster and you have connected to the primary unit.

   If the command output includes `Current HA mode: a-a, backup`, you have connected to a subordinate unit.

   If the command output includes `Current HA mode: standalone` the cluster unit is not operating in HA mode.
3. Enter the following command to confirm the HA configuration of the cluster:

```
get system ha status
```

```
Model: XXXX
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
Master:128 FGT_ha_2 FG600B3908600825 0
Slave :128 FGT_ha_1 FG600B3908600705 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG600B3908600825
Slave :1 FG600B3908600705
```

The command output shows both cluster units, their host names, their roles in the cluster, and their priorities. You can use this command to confirm that the cluster is operating normally. For example, if the command shows only one cluster unit then the other unit has left the cluster for some reason.

4. Use the `execute ha manage` command to connect to the other cluster unit's CLI and use these commands to verify cluster status.

To troubleshoot the cluster configuration

If the cluster members list and the dashboard does not display information for both cluster units the FortiGate units are not functioning as a cluster. See Troubleshooting full mesh HA on page 1419 to troubleshoot the cluster.

To add basic configuration settings and the redundant interfaces

Use the following steps to add a few basic configuration settings. Some steps use the CLI and some the web-based manager.

1. Log into the cluster CLI.
2. Add a password for the admin administrative account.

```
config system admin
   edit admin
      set password <password_str>
end
```

3. Temporarily delete the default route.

   You cannot add an interface to a redundant interface if any settings (such as the default route) are configured for it.

```
config router static
   delete 1
end
```

4. Go to **System > Network > Interface** and select **Create New** to add the redundant interface to connect to the Internet.
5. Add the redundant interface to connect to the Internet.

```
config system interface
   edit Port1_Port2
      set type redundant
      set member port1 port2
   end
```

6. Add the redundant interface to connect to the internal network.

```
config system interface
```

```
edit Port3_Port4
   set type redundant
   set member port3 port4
end
```

The virtual MAC addresses of the FortiGate interfaces change to the following. Note that port1 and port2 both have the port1 virtual MAC address and port3 and port4 both have the port3 virtual MAC address:

- port1 interface virtual MAC: `00-09-0f-09-00-00`
- port10 interface virtual MAC: `00-09-0f-09-00-01`
- port11 interface virtual MAC: `00-09-0f-09-00-02`
- port12 interface virtual MAC: `00-09-0f-09-00-03`
- port13 interface virtual MAC: `00-09-0f-09-00-04`
- port14 interface virtual MAC: `00-09-0f-09-00-05`
- port15 interface virtual MAC: `00-09-0f-09-00-06`
- port16 interface virtual MAC: `00-09-0f-09-00-07`
- port17 interface virtual MAC: `00-09-0f-09-00-08`
- port18 interface virtual MAC: `00-09-0f-09-00-09`
- port19 interface virtual MAC: `00-09-0f-09-00-0a`
- port2 interface virtual MAC: `00-09-0f-09-00-00` (same as port1)
- port20 interface virtual MAC: `00-09-0f-09-00-0c`
- port3 interface virtual MAC: `00-09-0f-09-00-0d`
- port4 interface virtual MAC: `00-09-0f-09-00-0d` (same as port3)
- port5 interface virtual MAC: `00-09-0f-09-00-0f`
- port6 interface virtual MAC: `00-09-0f-09-00-10`
- port7 interface virtual MAC: `00-09-0f-09-00-11`
- port8 interface virtual MAC: `00-09-0f-09-00-12`
- port9 interface virtual MAC: `00-09-0f-09-00-13`

7. Go to **Router > Static > Static Routes**.
8. Add the default route.

```
config router static
   edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 172.20.120.2
      set device Port1_Port2
end
```

To configure HA port monitoring for the redundant interfaces

1. Enter the following command to configure port monitoring for the redundant interfaces:

```
config system ha
   set monitor Port1_Port2 Port3_Port4
end
```

Troubleshooting full mesh HA

Troubleshooting full mesh HA clusters is similar to troubleshooting any cluster (see FGCP configuration examples and troubleshooting on page 1313 or Troubleshooting virtual clustering on page 1406). The configuration and

operation of a full mesh HA cluster is very similar to the configuration and operation of a standard cluster. The only differences relate to the configuration, connection, and operation of the redundant interfaces and redundant switches.

- Make sure the redundant interfaces and switches are connected correctly. With so many connections it is possible to make mistakes or for cables to become disconnected.
- Confirm that the configuration of the cluster unit 802.3ad Aggregate or Redundant interfaces is correct according to the configuration procedures in this chapter.
- In some configurations with some switch hardware, MAC-learning delays on the inter-switch links on the surrounding topologies may occur. The delays occur if the gratuitous ARP packets sent by the cluster after a failover are delayed by the switches before being sent across the inter-switch link. If this happens the surrounding topologies may be delayed in recognizing the failover and will keep sending packets to the MAC address of the failed primary unit resulting in lost traffic. Resolving this problem may require changing the configuration of the switch or replacing them with switch hardware that does not delay the gratuitous ARP packets.

Operating a cluster

With some exceptions, you can operate a cluster in much the same way as you operate a standalone FortiGate unit. This chapter describes those exceptions and also the similarities involved in operating a cluster instead of a standalone FortiGate unit.

Operating a cluster

The configurations of all of the FortiGate units in a cluster are synchronized so that the cluster units can simulate a single FortiGate unit. Because of this synchronization, you manage the HA cluster instead of managing the individual cluster units. You manage the cluster by connecting to the web-based manager using any cluster interface configured for HTTPS or HTTP administrative access. You can also manage the cluster by connecting to the CLI using any cluster interface configured for SSH or telnet administrative access.

The cluster web-based manager dashboard displays the cluster name, the host name and serial number of each cluster member, and also shows the role of each unit in the cluster. The roles can be master (primary unit) and slave (subordinate units). The dashboard also displays a cluster unit front panel illustration.

You can also go to **System > Config > HA** to view the cluster members list. This includes status information for each cluster unit. You can also use the cluster members list for a number of cluster management functions including changing the HA configuration of an operating cluster, changing the host name and device priority of a subordinate unit, and disconnecting a cluster unit from a cluster. See Cluster members list on page 1437.

You can use log messages to view information about the status of the cluster. SeeClusters and logging on page 1428. You can use SNMP to manage the cluster by configuring a cluster interface for SNMP administrative access. Using an SNMP manager you can get cluster configuration information and receive traps.

You can configure a reserved management interface to manage individual cluster units. You can use this interface to access the web-based manager or CLI and to configure SNMP management for individual cluster units. See Managing individual cluster units using a reserved management interface on page 1422.

You can manage individual cluster units by using SSH, telnet, or the CLI console on the web-based manager dashboard to connect to the CLI of the cluster. From the CLI you can use the `execute ha manage` command to connect to the CLI of any unit in the cluster.

You can also manage individual cluster units by using a null-modem cable to connect to any cluster unit CLI. From there you can use the `execute ha manage` command to connect to the CLI of each unit in the cluster.

Operating a virtual cluster

Managing a virtual cluster is very similar to managing a cluster that does not contain multiple virtual domains. Most of the information in this chapter applies to managing both kinds of clusters. This section describes what is different when managing a virtual cluster.

If virtual domains are enabled, the cluster web-based manager dashboard displays the cluster name and the role of each cluster unit in virtual cluster 1 and virtual cluster 2.

The configuration and maintenance options that you have when you connect to a virtual cluster web-based manager or CLI depend on the virtual domain that you connect to and the administrator account that you use to connect.

If you connect to a cluster as the administrator of a virtual domain, you connect directly to the virtual domain. Since HA virtual clustering is a global configuration, virtual domain administrators cannot see HA configuration options. However, virtual domain administrators see the host name of the cluster unit that they are connecting to on the web browser title bar or CLI prompt. This host name is the host name of the primary unit for the virtual domain. Also, when viewing log messages the virtual domain administrator can select to view log messages for either of the cluster units.

If you connect to a virtual cluster as the admin administrator you connect to the global web-based manager or CLI. Even so, you are connecting to an interface and to the virtual domain that the interface has been added to. The virtual domain that you connect to does not make a difference for most configuration and maintenance operations. However, there are a few exceptions. You connect to the FortiGate unit that functions as the primary unit for the virtual domain. So the host name displayed on the web browser title bar and on the CLI is the host name of this primary unit.

Managing individual cluster units using a reserved management interface

You can provide direct management access to all cluster units by reserving a management interface as part of the HA configuration. Once this management interface is reserved, you can configure a different IP address, administrative access and other interface settings for this interface for each cluster unit. Then by connecting this interface of each cluster unit to your network you can manage each cluster unit separately from a different IP address. Configuration changes to the reserved management interface are not synchronized to other cluster units.

The reserved management interface provides direct management access to each cluster unit and gives each cluster unit a different identity on your network. This simplifies using external services, such as SNMP, to separately monitor and manage each cluster unit.

The reserved management interface is not assigned an HA virtual MAC address like other cluster interfaces. Instead the reserved management interface retains the permanent hardware address of the physical interface unless you change it using the `config system interface` command.

The reserved management interface and IP address should not be used for managing a cluster using FortiManager. To correctly manage a FortiGate HA cluster with FortiManager use the IP address of one of the cluster unit interfaces.

If you enable SNMP administrative access for the reserved management interface you can use SNMP to monitor each cluster unit using the reserved management interface IP address. To monitor each cluster unit using SNMP, just add the IP address of each cluster unit's reserved management interface to the SNMP server configuration. You must also enable direct management of cluster members in the cluster SNMP configuration.

If you enable HTTPS or HTTP administrative access for the reserved management interfaces you can connect to the web-based manager of each cluster unit. Any configuration changes made to any of the cluster units is automatically synchronized to all cluster units. From the subordinate units the web-based manager has the same features as the primary unit except that unit-specific information is displayed for the subordinate unit, for example:

- The **Dashboard System Information** widget displays the subordinate unit serial number but also displays the same information about the cluster as the primary unit
- On the Cluster members list (go to **System > Config > HA**) you can change the HA configuration of the subordinate unit that you are logged into. For the primary unit and other subordinate units you can change only the host name and device priority.

- Log Access displays the logs of the subordinate that you are logged into fist, You use the HA Cluster list to view the log messages of other cluster units including the primary unit.

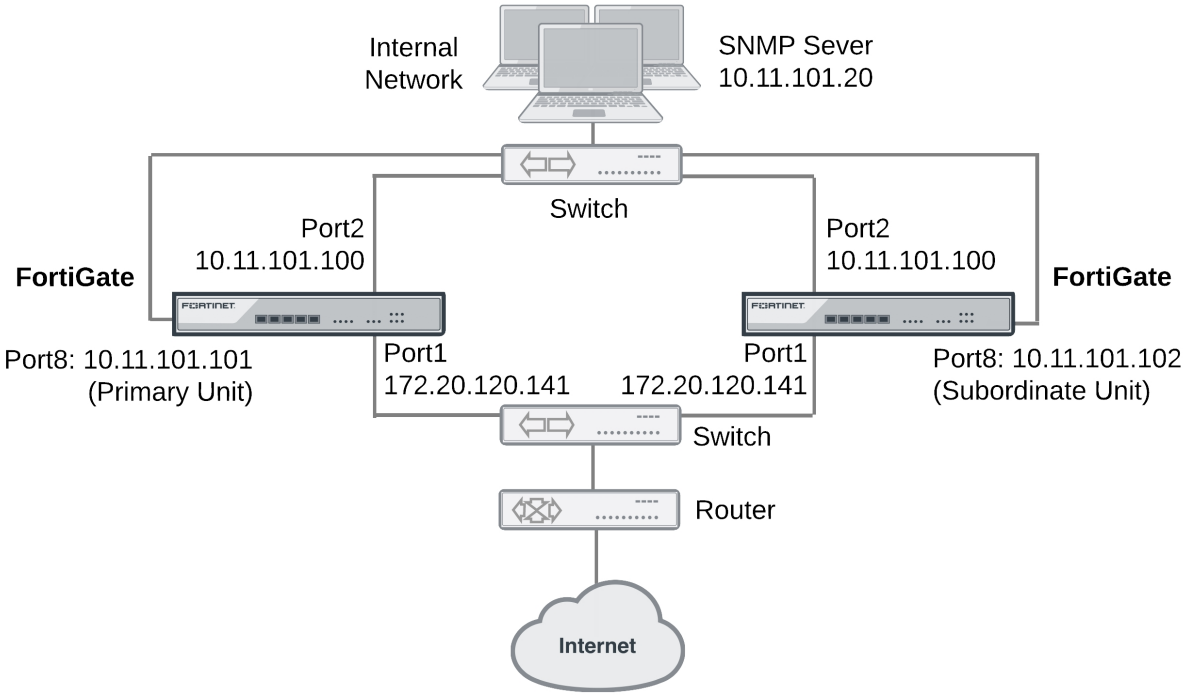
If you enable SSH or TELNET administrative access for the reserved management interfaces you can connect to the CLI of each cluster unit. The CLI prompt contains the host name of the cluster unit that you have connected to. Any configuration changes made to any of the cluster units is automatically synchronized to all cluster units. You can also use the `execute ha manage` command to connect to other cluster unit CLIs.

The reserved management interface is available in NAT/Route and in Transparent mode. It is also available if the cluster is operating with multiple VDOMs. In Transparent mode you cannot normally add an IP address to an interface. However, you can add an IP address to the reserved management interface.

Configuring the reserved management interface and SNMP remote management of individual cluster units

This example describes how to configure SNMP remote management of individual cluster units using the HA reserved management interface. The configuration consists of two FortiGate-620B units already operating as a cluster. In the example, the port8 interface of each cluster unit is connected to the internal network using the switch and configured as the reserved management interface.

SNMP remote management of individual cluster units



To configure the reserved management interface - web-based manager

1. Go to **System > Config > HA**.
2. Edit the primary unit.

3. Select **Reserve Management Port for Cluster Member** and select port8.
4. Select **OK**.

To configure the reserved management interface - CLI

From the CLI you can also configure IPv4 and IPv6 default routes that are only used by the reserved management interface.

1. Log into the CLI of any cluster unit.
2. Enter the following command to enable the reserved management interface, set port8 as the reserved interface, and add an IPv4 default route of 10.11.101.2 and an IPv6 default route of 2001:db8:0:2::20 for the reserved management interface.

```
config system ha
   set ha-mgmt-status enable
   set ha-mgmt-interface port8
   set ha-mgmt-interface-gateway 10.11.101.2
   set ha-mgmt-interface-gateway6 2001:db8:0:2::20
end
```

The reserved management interface default route is not synchronized to other cluster units.

To change the primary unit reserved management interface configuration - web-based manager

You can change the IP address of the primary unit reserved management interface from the primary unit web-based manager. Configuration changes to the reserved management interface are not synchronized to other cluster units.

1. From a PC on the internal network, browse to http://10.11.101.100 and log into the cluster web-based manager.
   This logs you into the primary unit web-based manager.

   You can identify the primary unit from its serial number or host name that appears on the System Information dashboard widget.
2. Go to **System > Network > Interfaces** and edit the port8 interface as follows:

Alias	primary_reserved
IP/Netmask	10.11.101.101/24
Administrative Access	Ping, SSH, HTTPS, SNMP

3. Select **OK**.
   You can now log into the primary unit web-based manager by browsing to https://10.11.101.101. You can also log into this primary unit CLI by using an SSH client to connect to 10.11.101.101.

To change subordinate unit reserved management interface configuration - CLI

At this point you cannot connect to the subordinate unit reserved management interface because it does not have an IP address. Instead, this procedure describes connecting to the primary unit CLI and using the `execute ha manage` command to connect to subordinate unit CLI to change the port8 interface. You can also use a serial connection to the cluster unit CLI. Configuration changes to the reserved management interface are not synchronized to other cluster units.

1. Connect to the primary unit CLI and use the `execute ha manage` command to connect to a subordinate unit CLI.

   You can identify the subordinate unit from is serial number or host name. The host name appears in the CLI prompt.

2. Enter the following command to change the port8 IP address to `10.11.101.102` and set management access to HTTPS, ping, SSH, and SNMP.

```
config system interface
   edit port8
      set ip 10.11.101.102/24
      set allowaccess https ping ssh snmp
end
```

   You can now log into the subordinate unit web-based manager by browsing to https://10.11.101.102. You can also log into this subordinate unit CLI by using an SSH client to connect to 10.11.101.102.

To configure the cluster for SNMP management using the reserved management interfaces - CLI

This procedure describes how to configure the cluster to allow the SNMP server to get status information from the primary unit and the subordinate unit. The SNMP configuration is synchronized to all cluster units. To support using the reserved management interfaces, you must add at least one HA direct management host to an SNMP community. If your SNMP configuration includes SNMP users with user names and passwords you must also enable HA direct management for SNMP users.

1. Enter the following command to add an SNMP community called `Community` and add a host to the community for the reserved management interface of each cluster unit. The host includes the IP address of the SNMP server (10.11.101.20).

```
config system snmp community
   edit 1
      set name Community
      config hosts
         edit 1
            set ha-direct enable
            set ip 10.11.101.20
         end
end
```

Enabling ha-direct in non-HA environments makes SNMP unusable.

2.

3. Enter the following command to add an SNMP user for the reserved management interface.

```
config system snmp user
   edit 1
      set ha-direct enable
      set notify-hosts 10.11.101.20
   end
```

   Configure other settings as required.

To get CPU, memory, and network usage of each cluster unit using the reserved management IP addresses

From the command line of an SNMP manager, you can use the following SNMP commands to get CPU, memory and network usage information for each cluster unit. In the examples, the community name is `Community`. The commands use the MIB field names and OIDs listed below.

Enter the following commands to get CPU, memory and network usage information for the primary unit with reserved management IP address 10.11.101.101 using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.101 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsNetUsage
```

Enter the following commands to get CPU, memory and network usage information for the primary unit with reserved management IP address 10.11.101.101 using the OIDs:

```
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

Enter the following commands to get CPU, memory and network usage information for the subordinate unit with reserved management IP address 10.11.101.102 using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.102 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsNetUsage
```

Enter the following commands to get CPU, memory and network usage information for the subordinate unit with reserved management IP address 10.11.101.102 using the OIDs:

```
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

Managing individual cluster units in a virtual cluster

You can select the HA option **Do NOT Synchronize Management VDOM Configuration** if you have enabled multiple VDOMS and set a VDOM other than the root VDOM to be the management VDOM. You can select this option to prevent the management VDOM configuration from being synchronized between cluster units in a virtual cluster. This allows you to add an interface to the VDOM in each cluster unit and then to give the interfaces different IP addresses in each cluster unit, allowing you to manage each cluster unit separately.

You can also enable this feature using the following command:

```
config system ha
   set standalone-mgmt-vdom enable
end
```

This feature must be disabled to manage a cluster using FortiManager.

The primary unit acts as a router for subordinate unit management traffic

HA uses routing and inter-VDOM links to route subordinate unit management traffic through the primary unit to the network. Similar to a standalone FortiGate unit, subordinate units may generate their own management traffic, including:

- DNS queries.
- FortiGuard Web Filtering rating requests.
- Log messages to be sent to a FortiAnalyzer unit, to a syslog server, or to the FortiGuard Analysis and Management Service.
- Log file uploads to a FortiAnalyzer unit.
- Quarantine file uploads to a FortiAnalyzer unit.
- SNMP traps.
- Communication with remote authentication servers (RADIUS, LDAP, TACACS+ and so on)

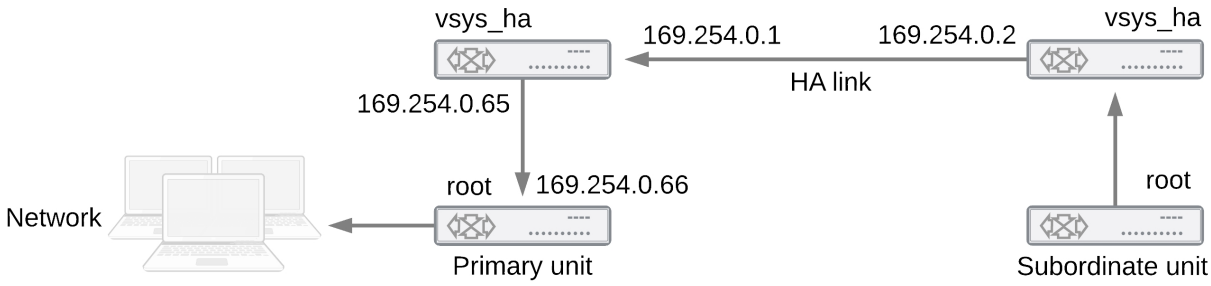
Subordinate units send this management traffic over the HA heartbeat link to the primary unit. The primary unit forwards the management traffic to its destination. The primary unit also routes replies back to the subordinate unit in the same way.

HA uses a hidden VDOM called vsys_ha for HA operations. The vsys_ha VDOM includes the HA heartbeat interfaces, and all communication over the HA heartbeat link goes through the vsys_ha VDOM. To provide communication from a subordinate unit to the network, HA adds hidden inter-VDOM links between the primary unit management VDOM and the primary unit vsys_ha VDOM. By default, root is the management VDOM.

Management traffic from the subordinate unit originates in the subordinate unit vsys_ha VDOM. The vsys_ha VDOM routes the management traffic over the HA heartbeat link to the primary unit vsys_ha VDOM. This management traffic is then routed to the primary unit management VDOM and from there out onto the network.

DNS queries and FortiGuard Web Filtering and Email Filter requests are still handled by the HA proxy so the primary unit and subordinate units share the same DNS query cache and the same FortiGuard Web Filtering and Email Filter cache. In a virtual clustering configuration, the cluster unit that is the primary unit for the management virtual domain maintains the FortiGuard Web Filtering, Email Filtering, and DNS query cache.

Subordinate unit management traffic path



Cluster communication with RADIUS and LDAP servers

In an active-passive cluster, only the primary unit processes traffic, so the primary unit communicates with RADIUS or LDAP servers. In a cluster that is operating in active-active mode, subordinate units send RADIUS and LDAP requests to the primary unit over the HA heartbeat link and the primary units routes them to their destination. The primary unit relays the responses back to the subordinate unit.

Clusters and FortiGuard services

This section describes how various FortiGate HA clustering configurations communicate with the FDN.

In an operating cluster, the primary unit communicates directly with the FortiGuard Distribution Network (FDN). Subordinate units also communicate directly with the FDN but as described above, all communication between subordinate units and the FDN is routed through the primary unit.

You must register and license all of the units in a cluster for all required FortiGuard services, both because all cluster units communicate with the FDN and because any cluster unit could potentially become the primary unit.

FortiGuard and active-passive clusters

For an active-passive cluster, only the primary unit processes traffic. Even so, all cluster units communicate with the FDN. Only the primary unit sends FortiGuard Web Filtering and Antispam requests to the FDN. All cluster units receive FortiGuard Antivirus, IPS, and application control updates from the FDN.

In an active-passive cluster the FortiGuard Web Filter and Email Filter caches are located on the primary unit in the same way as for a standalone FortiGate unit. The caches are not shared among cluster units so after a failover the new primary unit must build up new caches.

In an active-passive cluster all cluster units also communicate with the FortiGuard Analysis and Management Service (FAMS).

FortiGuard and active-active clusters

For an active-active cluster, both the primary unit and the subordinate units process traffic. Communication between the cluster units and the FDN is the same as for active-passive clusters with the following exception.

Because the subordinate units process traffic, they may also be making FortiGuard Web Filtering and Email Filter requests. The primary unit receives all such requests from the subordinate units and relays them to the FDN and then relays the FDN responses back to the subordinate units. The FortiGuard Web Filtering and Email Filtering URL caches are maintained on the primary unit. The primary unit caches are used for primary and subordinate unit requests.

FortiGuard and virtual clustering

For a virtual clustering configuration the management virtual domain of each cluster unit communicates with the FDN. The cluster unit that is the primary unit for the management virtual domain maintains the FortiGuard Web Filtering and Email Filtering caches. All FortiGuard Web Filtering and Email Filtering requests are proxied by the management VDOM of the cluster unit that is the primary unit for the management virtual domain.

Clusters and logging

This section describes the log messages that provide information about how HA is functioning, how to view and manage logs for each unit in a cluster, and provides some example log messages that are recorded during specific cluster events.

You configure logging for a cluster in the same way as you configuring logging for a standalone FortiGate unit. Log configuration changes made to the cluster are synchronized to all cluster units.

All cluster units record log messages separately to the individual cluster unit's log disk, to the cluster unit's system memory, or both. You can view and manage log messages for each cluster unit from the cluster web-based manager Log Access page.

When remote logging is configured, all cluster units send log messages to remote FortiAnalyzer units or other remote servers as configured. HA uses routing and inter-VDOM links to route subordinate unit log traffic through the primary unit to the network.

When you configure a FortiAnalyzer unit to receive log messages from a FortiGate cluster, you should add a cluster to the FortiAnalyzer unit configuration so that the FortiAnalyzer unit can receive log messages from all cluster units.

Viewing and managing log messages for individual cluster units

This section describes how to view and manage log messages for an individual cluster unit.

To view HA cluster log messages

1. Log into the cluster web-based manager.
2. Go to **Log&Report > Log Config > Log Settings > GUI Preferences** and select to display logs from **Memory**, **Disk or FortiAnalyzer**.
   For each log display, the **HA Cluster** list displays the serial number of the cluster unit for which log messages are displayed. The serial numbers are displayed in order in the list.
3. Set **HA Cluster** to the serial number of one of the cluster units to display log messages for that unit.

About HA event log messages

HA event log messages always include the host name and serial number of the cluster unit that recorded the message. HA event log messages also include the HA state of the unit and also indicate when a cluster unit switches (or moves) from one HA state to another. Cluster units can operate in the HA states listed below:

HA states

Hello	A FortiGate unit configured for HA operation has started up and is looking for other FortiGate units with which to form a cluster.
Work	In an active-passive cluster a cluster unit is operating as the primary unit. In an active-active cluster unit is operating as the primary unit or a subordinate unit.
Standby	In an active-passive cluster the cluster unit is operating as a subordinate unit.

HA log Event log messages also indicate the virtual cluster that the cluster unit is operating in as well as the member number of the unit in the cluster. If virtual domains are not enabled, all clusters unit are always operating in virtual cluster 1. If virtual domains are enabled, a cluster unit may be operating in virtual cluster 1 or virtual cluster 2. The member number indicates the position of the cluster unit in the cluster members list. Member 0 is the primary unit. Member 1 is the first subordinate unit, member 2 is the second subordinate unit, and so on.

HA log messages

See the FortiOS log message reference for a listing of and descriptions of the HA log messages.

FortiGate HA message "HA master heartbeat interface <intf_name> lost neighbor information"

The following HA log messages may be recorded by an operating cluster:

2009-02-16 11:06:34 device_id=FG2001111111 log_id=0105035001 type=event subtype=ha pri=critical vd=root msg="HA slave heartbeat interface internal lost neighbor information"

2009-02-16 11:06:40 device_id=FG2001111111 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Virtual cluster 1 of group 0 detected new joined HA member"

2009-02-16 11:06:40 device_id=FG2001111111 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA master heartbeat interface internal get peer information"

These log messages indicate that the cluster units could not connect to each other over the HA heartbeat link for the period of time that is given by hb-interval x hb-lost-threshold, which is 1.2 seconds with the default values.

To diagnose this problem

1. Check all heartbeat interface connections including cables and switches to make sure they are connected and operating normally.
2. Use the following commands to display the status of the heartbeat interfaces.

   ```
   get hardware nic <heartbeat_interface_name>
   diagnose hardware deviceinfo nic <heartbeat_interface_name>
   ```

   The status information may indicate the interface status and link status and also indicate if a large number of errors have been detected.
3. If the log message only appears during peak traffic times, increase the tolerance for missed HA heartbeat packets by using the following commands to increase the lost heartbeat threshold and heartbeat interval:

   ```
   config system ha
      set hb-lost-threshold 12
      set hb-interval 4
   end
   ```

   These settings multiply by 4 the loss detection interval. You can use higher values as well.

   This condition can also occur if the cluster units are located in different buildings or even different geographical locations. Called a distributed cluster, as a result of the separation it may take a relatively long time for heartbeat packets to be transmitted between cluster units. You can support a distributed cluster by increasing the heartbeat interval so that the cluster expects extra time between heartbeat packets.
4. Optionally disable session-pickup to reduce the processing load on the heartbeat interfaces.
5. Instead of disabling session-pickup you can enable `session-pickup-delay` to reduce the number of sessions that are synchronized. With this option enabled only sessions that are active for more than 30 seconds are synchronized.

It may be useful to monitor CPU and memory usage to check for low memory and high CPU usage. You can configure event logging to monitor CPU and memory usage. You can also enable the CPU over usage and memory low SNMP events.

Once this monitoring is in place, try and determine if there have been any changes in the network or an increase of traffic recently that could be the cause. Check to see if the problem happens frequently and if so what the pattern is.

To monitor the CPU of the cluster units and troubleshoot further, use the following procedure and commands:

```
get system performance status
get system performance top 2
diagnose sys top 2
```

These commands repeated at frequent intervals will show the activity of the CPU and the number of sessions.

Search the Fortinet Knowledge Base for articles about monitoring CPU and Memory usage.

If the problem persists, gather the following information (a console connection might be necessary if connectivity is lost) and provide it to Technical Support when opening a ticket:

- Debug log from the web-based manager: **System > Config > Advanced > Download Debug Log**
- CLI command output:

```
diagnose sys top 2 (keep it running for 20 seconds)
get system performance status (repeat this command multiple times to get good samples)
get system ha status
diagnose sys ha status
diagnose sys ha dump-by {all options}
diagnose netlink device list
diagnose hardware deviceinfo nic <heartbeat-interface-name>
execute log filter category 1
execute log display
```

Formatting cluster unit hard disks (log disks)

If you need to format the hard disk (also called log disk or disk storage) of one or more cluster units you should disconnect the unit from the cluster and use the `execute formatlogdisk` command to format the cluster unit hard disk then add the unit back to the cluster.

For information about how to remove a unit from a cluster and add it back, see Disconnecting a cluster unit from a cluster on page 1451 and Adding a disconnected FortiGate unit back to its cluster on page 1452 .

Once you add the cluster unit with the formatted log disk back to the cluster you should make it the primary unit before removing other units from the cluster to format their log disks and then add them back to the cluster.

Clusters and SNMP

You can use SNMP to manage a cluster by configuring a cluster interface for SNMP administrative access. Using an SNMP manager you can get cluster configuration and status information and receive traps.

You configure SNMP for a cluster in the same way as configuring SNMP for a standalone FortiGate unit. SNMP configuration changes made to the cluster are shared by all cluster units.

Each cluster unit sends its own traps and SNMP manager systems can use SNMP get commands to query each cluster unit separately. To set SNMP get queries to each cluster unit you must create a special get command that includes the serial number of the cluster unit.

Alternatively you can use the HA reserved management interface feature to give each cluster unit a different management IP address. Then you can create an SNMP get command for each cluster unit that just includes the management IP address and does not have to include the serial number.

SNMP get command syntax for the primary unit

Normally, to get configuration and status information for a standalone FortiGate unit or for a primary unit, an SNMP manager would use an SNMP get commands to get the information in a MIB field. The SNMP get command syntax would be similar to the following:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. The most commonly used community name is `public`.

`<address_ipv4>` is the IP address of the FortiGate interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself. The HA MIB fields and OIDs are listed below:

SNMP field names and OIDs

MIB field	OID	Description
fgHaSystemMode	.1.3.6.1.4.1.12356.101.13.1.1.0	HA mode (standalone, a-a, or a-p)
fgHaGroupId	.1.3.6.1.4.1.12356.101.13.1.2.0	The HA priority of the cluster unit. Default 128.
fgHaPriority	.1.3.6.1.4.1.12356.101.13.1.3.0	The HA priority of the cluster unit. Default 128.
fgHaOverride	.1.3.6.1.4.1.12356.101.13.1.4.0	Whether HA override is disabled or enabled for the cluster unit.
fgHaAutoSync	.1.3.6.1.4.1.12356.101.13.1.5.0	Whether automatic HA synchronization is disabled or enabled.
fgHaSchedule	.1.3.6.1.4.1.12356.101.13.1.6.0	The HA load balancing schedule. Set to none unless operating in a-p mode.
fgHaGroupName	.1.3.6.1.4.1.12356.101.13.1.7.0	The HA group name.
fgHaStatsIndex	.1.3.6.1.4.1.12356.101.13.2.1.1.1.1	The cluster index of the cluster unit. 1 for the primary unit, 2 to x for the subordinate units.
fgHaStatsSerial	.1.3.6.1.4.1.12356.101.13.2.1.1.2.1	The serial number of the cluster unit.
fgHaStatsCpuUsage	.1.3.6.1.4.1.12356.101.13.2.1.1.3.1	The cluster unit's current CPU usage.
fgHaStatsMemUsage	.1.3.6.1.4.1.12356.101.13.2.1.1.4.1	The cluster unit's current Memory usage.
fgHaStatsNetUsage	.1.3.6.1.4.1.12356.101.13.2.1.1.5.1	The cluster unit's current Network bandwidth usage.
fgHaStatsSesCount	.1.3.6.1.4.1.12356.101.13.2.1.1.6.1	The cluster unit's current session count.
fgHaStatsPktCount	.1.3.6.1.4.1.12356.101.13.2.1.1.7.1	The cluster unit's current packet count.
fgHaStatsByteCount	.1.3.6.1.4.1.12356.101.13.2.1.1.8.1	The cluster unit's current byte count.
fgHaStatsIdsCount	.1.3.6.1.4.1.12356.101.13.2.1.1.9.1	The number of attacks reported by the IPS for the cluster unit.
fgHaStatsAvCount	.1.3.6.1.4.1.12356.101.13.2.1.1.10.1	The number of viruses reported by the anti-virus system for the cluster unit.
fgHaStatsHostname	.1.3.6.1.4.1.12356.101.13.2.1.1.11.1	The hostname of the cluster unit.

To get the HA priority for the primary unit

The following SNMP get command gets the HA priority for the primary unit. The community name is `public`. The IP address of the cluster interface configured for SNMP management access is 10.10.10.1. The HA priority MIB field is fgHaPriority and the OID for this MIB field is 1.3.6.1.4.1.12356.101.13.1.3.0 The first command uses the MIB field name and the second uses the OID:

```
snmpget -v2c -c public 10.10.10.1 fgHaPriority
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.13.1.3.0
```

SNMP get command syntax for any cluster unit

To get configuration status information for a specific cluster unit (for the primary unit or for any subordinate unit), the SNMP manager must add the serial number of the cluster unit to the SNMP get command after the community name. The community name and the serial number are separated with a dash. The syntax for this SNMP get command would be:

```
snmpget -v2c -c <community_name>-<fgt_serial> <address_ipv4> {<OID> | <MIB_field>}
```

where:

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. All units in the cluster have the same community name. The most commonly used community name is `public`.

`<fgt_serial>` is the serial number of any cluster unit. For example, FGT4002803033172. You can specify the serial number of any cluster unit, including the primary unit, to get information for that unit.

`<address_ipv4>` is the IP address of the FortiGate interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself.

If the serial number matches the serial number of a subordinate unit, the SNMP get request is sent over the HA heartbeat link to the subordinate unit. After processing the request, the subordinate unit sends the reply back over the HA heartbeat link back to the primary unit. The primary unit then forwards the response back to the SNMP manager.

If the serial number matches the serial number of the primary unit, the SNMP get request is processed by the primary unit. You can actually add a serial number to the community name of any SNMP get request. But normally you only need to do this for getting information from a subordinate unit.

To get the CPU usage for a subordinate unit

The following SNMP get command gets the CPU usage for a subordinate unit in a FortiGate-5001SX cluster. The subordinate unit has serial number FG50012205400050. The community name is `public`. The IP address of the FortiGate interface is 10.10.10.1. The HA status table MIB field is fgHaStatsCpuUsage and the OID for this MIB field is 1.3.6.1.4.1.12356.101.13.2.1.1.3.1. The first command uses the MIB field name and the second uses the OID for this table:

```
snmpget -v2c -c public-FG50012205400050 10.10.10.1 fgHaStatsCpuUsage
snmpget -v2c -c public-FG50012205400050 10.10.10.1 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
```

FortiGate SNMP recognizes the community name with syntax `<community_name>-<fgt_serial>`. When the primary unit receives an SNMP get request that includes the community name followed by serial number, the FGCP extracts the serial number from the request. Then the primary unit redirects the SNMP get request to the cluster unit with that serial number. If the serial number matches the serial number of the primary unit, the SNMP get is processed by the primary unit.

Getting serial numbers of cluster units

The following SNMP get commands use the MIB field name fgHaStatsSerial.<index> to get the serial number of each cluster unit. Where <index> is the cluster unit's cluster index and 1 is the cluster index of the primary unit, 2 is the cluster index of the first subordinate unit, and 3 is the cluster index of the second subordinate unit.

The OID for this MIB field is `1.3.6.1.4.1.12356.101.13.2.1.1.2.1`. The community name is `public`. The IP address of the FortiGate interface is 10.10.10.1.

The first command uses the MIB field name and the second uses the OID for this table and gets the serial number of the primary unit:

```
snmpget -v2c -c public 10.10.10.1 fgHaStatsSerial.1
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.13.2.1.1.2.1
```

The second command uses the MIB field name and the second uses the OID for this table and gets the serial number of the first subordinate unit:

```
snmpget -v2c -c public 10.10.10.1 fgHaStatsSerial.2
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.13.2.2.2
```

SNMP get command syntax - reserved management interface enabled

To get configuration and status information for any cluster unit where you have enabled the HA reserved management interface feature and assigned IP addresses to the management interface of each cluster unit, an SNMP manager would use the following get command syntax:

```
snmpget -v2c -c <community_name> <mgmt_address_ipv4> {<OID> | <MIB_field>}
```

where:

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community names to a FortiGate SNMP configuration. The most commonly used community name is `public`.

`<mgmt_address_ipv4>` is the IP address of the FortiGate HA reserved management interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself. To find OIDs and MIB field names see your FortiGate unit's online help.

Adding FortiClient licenses to a cluster

Each FortiGate unit in a cluster must have its own FortiClient license. Contact your reseller to purchase FortiClient licenses for all of the FortiGate units in your cluster.

When you receive the license keys you can log into the Fortinet Support site and add the FortiClient license keys to each FortiGate unit. Then, as long as the cluster can connect to the Internet each cluster unit receives its FortiClient license key from the FortiGuard network.

Adding FortiClient licenses to cluster units with a reserved management interface

You can also use the following steps to manually add license keys to your cluster units from the web-based manager or CLI. Your cluster must be connected to the Internet and you must have configured a reserved management interface for each cluster unit.

1. Log into the -web-based manager of each cluster unit using its reserved management interface IP address.
2. Go to the **License Information** dashboard widget and beside **FortiClient** select **Enter License**.

3. Enter the license key and select **OK**.
4. Confirm that the license has been installed and the correct number of FortiClients are licensed.
5. Repeat for all of the cluster units.

You can also use the reserved management IP address to log into each cluster unit CLI and use following command to add the license key:

```
execute FortiClient-NAC update-registration-license <license-key>
```

You can connect to the CLIs of each cluster unit using their reserved management IP address.

Adding FortiClient licenses to cluster units with no reserved management interface

If you have not set up reserved management IP addresses for your cluster units, you can still add FortiClient license keys to each cluster unit. You must log into the primary unit and then use the `execute ha manage` command to connect to each cluster unit CLI. For example, use the following steps to add a FortiClient license key a cluster of three FortiGate units:

1. Log into the primary unit CLI and enter the following command to confirm the serial number of the primary unit:
   ```
   get system status
   ```
2. Add the FortiClient license key for that serial number to the primary unit:
   ```
   execute FortiClient-NAC update-registration-license <license-key>
   ```
   You can also use the web-based manager to add the license key to the primary unit.
3. Enter the following command to log into the first subordinate unit:
   ```
   execute ha manage 1
   ```
4. Enter the following command to confirm the serial number of the cluster unit that you have logged into:
   ```
   get system status
   ```
5. Add the FortiClient license key for that serial number to the cluster unit:
   ```
   execute FortiClient-NAC update-registration-license <license-key>
   ```
6. Enter the following command to log into the second subordinate unit:
   ```
   execute ha manage 2
   ```
7. Enter the following command to confirm the serial number of the cluster unit that you have logged into:
   ```
   get system status
   ```
8. Add the FortiClient license key for that serial number to the cluster unit:
   ```
   execute FortiClient-NAC update-registration-license <license-key>
   ```

Viewing FortiClient license status and active FortiClient users for each cluster unit

To view FortiClient license status and FortiClient information for each cluster unit you must log into each cluster unit's web-based manager or CLI. You can do this by connecting to each cluster unit's reserved management interface if they are configured. If you have not configured reserved management interfaces you can use the execute ha manage command to log into each cluster unit CLI.

From the web-based manager, view FortiClient License status from the License Information dashboard widget and select **Details** to display the list of active FortiClient users connecting through that cluster unit. You can also see active FortiClient users by going to **User & Device > Monitor > FortiClient**.

From the CLI you can use the `execute FortiClient {list | info}` command to display FortiClient license status and active FortiClient users.

For example, use the following command to display the FortiClient license status of the cluster unit that you are logged into:

```
execute forticlient info
Maximum FortiClient connections: unlimited.
Licensed connections: 114
   NAC: 114
WANOPT: 0
Test: 0
Other connections:
   IPsec: 0
   SSLVPN: 0
```

Use the following command to display the list of active FortiClient users connecting through the cluster unit. The output shows the time the connection was established, the type of FortiClient connection, the name of the device, the user name of the person connecting, the FortiClient ID, the host operating system, and the source IP address of the session.

```
execute forticlient list
TIMESTAMP TYPE CONNECT-NAME USER CLIENT-ID HOST-OS SRC-IP
   20141017 09:13:33 NAC Gordon-PC Gordon 11F76E902611484A942E31439E428C5C Microsoft
       Windows 7 , 64-bit Service Pack 1 (build 7601) 172.20.120.10
   20141017 09:11:55 NAC Gordon-PC 11F76E902611484A942E31439E428C5C Microsoft Windows 7 ,
       64-bit Service Pack 1 (build 7601) 172.20.120.10
   20141017 07:27:11 NAC Desktop11 Richie 9451C0B8EE3740AEB7019E920BB3761B Microsoft
       Windows 7, 64-bit Service Pack 1 (build 7601) 172.20.120.20
```

Cluster members list

To display the cluster members list, go to **System > Config > HA**.

The cluster members list displays illustrations of the front panels of the cluster units. If the network jack for an interface is shaded green, the interface is connected. Hover the mouse pointer over each illustration to view the cluster unit host name, serial number, and how long the unit has been operating (up time). The list of monitored interfaces is also displayed.

From the cluster members list you can:

- View HA statistics.
- Use the up and down arrows to change the order in which cluster units are listed.
- See the host name of each cluster unit. To change the primary unit host name, go to the system dashboard and select Change beside the current host name in the System Information widget. To view and change a subordinate unit host name, from the cluster members list select the edit icon for a subordinate unit.
- View the status or role of each cluster unit.
- View and optionally change the HA configuration of the operating cluster.
- View and optionally change the host name and device priority of a subordinate unit.
- Disconnect a cluster unit from a cluster.
- Download the Debug log for any cluster unit. You can send this debug log file to Fortinet Technical Support to help diagnose problems with the cluster or with individual cluster units.

Virtual cluster members list

If virtual domains are enabled, you can display the cluster members list to view the status of the operating virtual clusters. The virtual cluster members list shows the status of both virtual clusters including the virtual domains added to each virtual cluster.

To display the virtual cluster members list for an operating cluster log in as the admin administrator, select Global Configuration and go to **System > Config > HA**.

The functions of the virtual cluster members list are the same as the functions of the Cluster Members list with the following exceptions.

- When you select the edit icon for a primary unit in a virtual cluster, you can change the virtual cluster 1 and virtual cluster 2 device priority of this cluster unit and you can edit the VDOM partitioning configuration of the cluster.
- When you select the edit icon for a subordinate unit in a virtual cluster, you can change the device priority for the subordinate unit for the selected virtual cluster.

Also, the HA cluster members list changes depending on the cluster unit that you connect to.

Viewing HA statistics

From the cluster members list you can select **View HA statistics** to display the serial number, status, and monitor information for each cluster unit. To view HA statistics, go to **System > Config > HA** and select View HA Statistics. Note the following about the HA statistics display:

- Use the serial number ID to identify each FortiGate unit in the cluster. The cluster ID matches the FortiGate unit serial number.
- Status indicates the status of each cluster unit. A green check mark indicates that the cluster unit is operating normally. A red X indicates that the cluster unit cannot communicate with the primary unit.
- The up time is the time in days, hours, minutes, and seconds since the cluster unit was last started.
- The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
- The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

Changing the HA configuration of an operating cluster

To change the configuration settings of an operating cluster, go to **System > Config > HA** to display the cluster members list. Select Edit for the master (or primary) unit in the cluster members list to display the HA configuration page for the cluster.

You can use the HA configuration page to check and fine tune the configuration of the cluster after the cluster is up and running. For example, if you connect or disconnect cluster interfaces you may want to change the Port Monitor configuration.

Any changes you make on this page, with the exception of changes to the device priority, are first made to the primary unit configuration and then synchronized to the subordinate units. Changing the device priority only affects the primary unit.

Changing the HA configuration of an operating virtual cluster

To change the configuration settings of the primary unit in a functioning cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to **System > Config > HA** to display the cluster members list. Select Edit for the master (or primary) unit in virtual cluster 1 or virtual cluster 2 to display the HA configuration page for the virtual cluster.

You can use the virtual cluster HA configuration page to check and fine tune the configuration of both virtual clusters after the cluster is up and running. For example, you may want to change the Port Monitor configuration for virtual cluster 1 and virtual cluster 2 so that each virtual cluster monitors its own interfaces.

You can also use this configuration page to move virtual domains between virtual cluster 1 and virtual cluster 2. Usually you would distribute virtual domains between the two virtual clusters to balance the amount of traffic being processed by each virtual cluster.

Any changes you make on this page, with the exception of changes to the device priorities, are first made to the primary unit configuration and then synchronized to the subordinate unit.

You can also adjust device priorities to configure the role of this cluster unit in the virtual cluster. For example, to distribute traffic to both cluster units in the virtual cluster configuration, you would want one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. You can create this configuration by setting the device priorities. The cluster unit with the highest device priority in virtual cluster 1 becomes the primary unit for virtual cluster 1. The cluster unit with the highest device priority in virtual cluster 2 becomes the primary unit in virtual cluster 2.

Changing the subordinate unit host name and device priority

To change the host name and device priority of a subordinate unit in an operating cluster, go to **System > Config > HA** to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

To change the host name and device priority of a subordinate unit in an operating cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to **System > Config > HA** to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

You can change the host name (Peer) and device priority (Priority) of this subordinate unit. These changes only affect the configuration of the subordinate unit.

The device priority is not synchronized among cluster members. In a functioning cluster you can change device priority to change the priority of any unit in the cluster. The next time the cluster negotiates, the cluster unit with the highest device priority becomes the primary unit.

The device priority range is 0 to 255. The default device priority is 128.

Upgrading cluster firmware

You can upgrade the FortiOS firmware running on an HA cluster in the same manner as upgrading the firmware running on a standalone FortiGate unit. During a normal firmware upgrade, the cluster upgrades the primary unit and all subordinate units to run the new firmware image. The firmware upgrade takes place without interrupting communication through the cluster.

Upgrading cluster firmware to a new major release (for example upgrading from 5.0 MRx to 5.2.2) is supported for clusters. Make sure you are taking an upgrade path described in the release notes. Even so you should back up your configuration and only perform such a firmware upgrade during a maintenance window.

To upgrade the firmware without interrupting communication through the cluster, the cluster goes through a series of steps that involve first upgrading the firmware running on the subordinate units, then making one of the subordinate units the primary unit, and finally upgrading the firmware on the former primary unit. These steps are transparent to the user and the network, but depending upon your HA configuration may result in the cluster selecting a new primary unit.

The following sequence describes in detail the steps the cluster goes through during a firmware upgrade and how different HA configuration settings may affect the outcome.

1. The administrator uploads a new firmware image from the web-based manager or CLI.
2. If the cluster is operating in active-active mode load balancing is turned off.
3. The cluster upgrades the firmware running on all of the subordinate units.
4. Once the subordinate units have been upgraded, a new primary unit is selected.

   This primary unit will be running the new upgraded firmware.
5. The cluster now upgrades the firmware of the former primary unit.

   If the age of the new primary unit is more than 300 seconds (5 minutes) greater than the age of all other cluster units, the new primary unit continues to operate as the primary unit.

   This is the intended behavior but does not usually occur because the age difference of the cluster units is usually less than the cluster age difference margin of 300 seconds. So instead, the cluster negotiates again to select a primary unit as described in An introduction to the FGCP on page 1270.

   You can keep the cluster from negotiating again by reducing the cluster age difference margin using the `ha-uptime-diff-margin` option. However, you should be cautious when reducing the age or other problems may occur. For information about the cluster age difference margin, see An introduction to the FGCP on page 1270. For more information about changing the cluster age margin, see An introduction to the FGCP on page 1270.
6. If the cluster is operating in active-active mode, load balancing is turned back on.

Changing how the cluster processes firmware upgrades

By default cluster firmware upgrades proceed as uninterruptable upgrades that do not interrupt traffic flow. If required, you can use the following CLI command to change how the cluster handles firmware upgrades. You might want to change this setting if you are finding uninterruptable upgrades take too much time.

```
config system ha
   set uninterruptible-upgrade disable
end
```

`uninterruptible-upgrade` is enabled by default. If you disable `uninterruptible-upgrade` the cluster still upgrades the firmware on all cluster units, but all cluster units are upgraded at once; which takes less time but interrupts communication through the cluster.

Synchronizing the firmware build running on a new cluster unit

If the firmware build running on a FortiGate unit that you add to a cluster is older than the cluster firmware build, you may be able to use the following steps to synchronize the firmware running on the new cluster unit.

This procedure describes re-installing the same firmware build on a cluster to force the cluster to upgrade all cluster units to the same firmware build.

Due to firmware upgrade and synchronization issues, in some cases this procedure may not work. In all cases it will work to install the same firmware build on the new unit as the one that the cluster is running before adding the new unit to the cluster.

To synchronize the firmware build running on a new cluster unit

1. Obtain a firmware image that is the same as build already running on the cluster.
2. Connect to the cluster using the web-based manager.
3. Go to the **System Information** dashboard widget.
4. Select **Update** beside **Firmware Version**.
   You can also install a newer firmware build.
5. Select **OK**.
   After the firmware image is uploaded to the cluster, the primary unit upgrades all cluster units to this firmware build.

Downgrading cluster firmware

For various reasons you may need to downgrade the firmware that a cluster is running. You can use the information in this section to downgrade the firmware version running on a cluster.

In most cases you can downgrade the firmware on an operating cluster using the same steps as for a firmware upgrade. A warning message appears during the downgrade but the downgrade usually works and after the downgrade the cluster continues operating normally with the older firmware image.

Downgrading between some firmware versions, especially if features have changed between the two versions, may not always work without the requirement to fix configuration issues after the downgrade.

Only perform firmware downgrades during maintenance windows and make sure you back up your cluster configuration before the downgrade.

If the firmware downgrade that you are planning may not work without configuration loss or other problems, you can use the following downgrade procedure to make sure your configuration is not lost after the downgrade.

To downgrade cluster firmware

This example shows how to downgrade the cluster shown in Example NAT/Route mode HA network topology. The cluster consists of two cluster units (FGT_ha_1 and FGT_ha_2). The port1 and port2 interfaces are connected to networks and the port3 and port4 interfaces are connected together for the HA heartbeat.

This example, describes separating each unit from the cluster and downgrading the firmware for the standalone FortiGate units. There are several ways you could disconnect units from the cluster. This example describes using the disconnect from cluster function on the cluster members list GUI page.

1. Go to the **System Information** dashboard widget and backup the cluster configuration.
   From the CLI use `execute backup config`.
2. Go to **System > Config > HA** and for FGT_ha_1 select the **Disconnect from cluster** icon.
3. Select the port2 interface and enter an IP address and netmask of 10.11.101.101/24 and select **OK**.
   From the CLI you can enter the following command (FG600B3908600705 is the serial number of the

cluster unit) to be able to manage the standalone FortiGate unit by connecting to the port2 interface with IP address and netmask 10.11.101.101/24.

```
execute ha disconnect FG600B3908600705 port2 10.11.101.101/24
```

After FGT_ha_1 is disconnected, FGT_ha_2 continues processing traffic.

4. Connect to the FGT_ha_1 web-based manager or CLI using IP address 10.11.101.101/24 and follow normal procedures to downgrade standalone FortiGate unit firmware.
5. When the downgrade is complete confirm that the configuration of 620_ha_1 is correct.
6. Set the HA mode of FGT_ha_2 to Standalone and follow normal procedures to downgrade standalone FortiGate unit firmware.

   Network communication will be interrupted for a short time during the downgrade.
7. When the downgrade is complete confirm that the configuration of FGT_ha_2 is correct.
8. Set the HA mode of FGT_ha_2 to Active-Passive or the required HA mode.
9. Set the HA mode of FGT_ha_1 to the same mode as FGT_ha_2.

   If you have not otherwise changed the HA settings of the cluster units and if the firmware downgrades have not affected the configurations the units should negotiate and form cluster running the downgraded firmware.

Backing up and restoring the cluster configuration

You can backup the configuration of the primary unit by logging into the web-based manager or CLI and following normal configuration backup procedures.

The following configuration settings are not synchronized to all cluster units:

- HA override and priority
- The interface configuration of the HA reserved management interface (`config system interface`)
- The HA reserved management interface default IPv4 route (`ha-mgmt-interface-gateway`)
- The HA reserved management interface default IPv6 route (`ha-mgmt-interface-gateway6`)
- The FortiGate unit host name.

To backup these configuration settings for each cluster unit you must log into each cluster unit and backup its configuration.

If you need to restore the configuration of the cluster including the configuration settings that are not synchronized you should first restore the configuration of the primary unit and then restore the configuration of each cluster unit. Alternatively you could log into each cluster unit and manually add the configuration settings that were not restored.

Monitoring cluster units for failover

If the primary unit in the cluster fails, the units in the cluster renegotiate to select a new primary unit. Failure of the primary unit results in the following:

- If SNMP is enabled, the new primary unit sends HA trap messages. The messages indicate a cluster status change, HA heartbeat failure, and HA member down.
- If event logging is enabled and HA activity event is selected, the new primary unit records log messages that show that the unit has become the primary unit.

- If alert email is configured to send email for HA activity events, the new primary unit sends an alert email containing the log message recorded by the event log.
- The cluster contains fewer FortiGate units. The failed primary unit no longer appears on the Cluster Members list.
- The host name and serial number of the primary unit changes. You can see these changes when you log into the web-based manager or CLI.
- The cluster info displayed on the dashboard, cluster members list or from the `get system ha status` command changes.

If a subordinate unit fails, the cluster continues to function normally. Failure of a subordinate unit results in the following:

- If event logging is enabled and HA activity event is selected, the primary unit records log messages that show that a subordinate has been removed from the cluster.
- If alert email is configured to send email for HA activity events, the new primary unit sends an alert email containing the log message recorded by the event log.
- The cluster contains fewer FortiGate units. The failed unit no longer appears on the Cluster Members list.

Viewing cluster status from the CLI

Use the `get system ha status` command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

The command display includes the following fields.

Fields	Description
`Model`	The FortiGate model number.
`Mode`	The HA mode of the cluster: a-a or a-p.
`Group`	The group ID of the cluster.
`Debug`	The debug status of the cluster.
`ses_pickup`	The status of session pickup: enable or disable.
`load balance`	The status of the `load-balance-all` keyword: enable or disable. Relevant to active-active clusters only.
`schedule`	The active-active load balancing schedule. Relevant to active-active clusters only.
`Master Slave`	`Master` displays the device priority, host name, serial number, and cluster index of the primary (or master) unit. `Slave` displays the device priority, host name, serial number, and cluster index of the subordinate (or slave, or backup) unit or units. The list of cluster units changes depending on how you log into the CLI. Usually you would use SSH or telnet to log into the primary unit CLI. In this case the primary unit would be at the top the list followed by the other cluster units. If you use `execute ha manage` or a console connection to log into a subordinate unit CLI, and then enter `get system ha status` the subordinate unit that you have logged into appears at the top of the list of cluster units.
`number of vcluster`	The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters.

Fields	Description
	The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, `vcluster 1` displays information for the cluster. If virtual domains are enabled, `vcluster 1` displays information for virtual cluster 1. The HA heartbeat IP address is 169.254.0.2 if you are logged into the primary unit of virtual cluster 1 and 169.254.0.1 if you are logged into a subordinate unit of virtual cluster 1. `vcluster 1` also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list.
`vcluster 1` `Master Slave`	If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit. If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into. If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit. If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into.
`vcluster 2` `Master Slave`	`vcluster 2` only appears if virtual domains are enabled. `vcluster 2` displays the HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 2. The HA heartbeat IP address is 169.254.0.2 if you are logged into the primary unit of virtual cluster 2 and 169.254.0.1 if you are logged into a subordinate unit of virtual cluster 2. `vcluster 2` also lists the primary unit (master) and subordinate units (slave) in virtual cluster 2. The list includes the cluster index and serial number of each cluster unit in virtual cluster 2. The cluster unit that you have logged into is at the top of the list. If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is `work`. The display lists the cluster units starting with the virtual cluster 2 primary unit. If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is `standby`. The display lists the cluster units starting with the subordinate unit that you are logged into.

Examples

The following example shows `get system ha status` output for a cluster of two FortiGate-5001SX units operating in active-active mode. The cluster group ID, session pickup, load balance all, and the load balancing schedule are all set to the default values. The device priority of the primary unit is also set to the default value. The device priority of the subordinate unit has been reduced to 100. The host name of the primary unit is `5001_Slot_4`. The host name of the subordinate unit in is `5001_Slot_3`.

The command output was produced by connecting to the primary unit CLI (host name `5001_Slot_4`).

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4 FG50012204400045 1
Slave :100 5001_Slot_3 FG50012205400050 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FG50012204400045
Slave :1 FG50012205400050
```

The following command output was produced by using `execute HA manage 0` to log into the subordinate unit CLI of the cluster shown in the previous example. The host name of the subordinate unit is `5001_Slot_3`.

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Slave :100 5001_Slot_3 FG50012205400050 0
Master:128 5001_Slot_4 FG50012204400045 1
number of vcluster: 1
vcluster 1: work 169.254.0.2
Slave :1 FG50012205400050
Master:0 FG50012204400045
```

The following example shows `get system ha status` output for a cluster of three FortiGate-5001 units operating in active-passive mode. The cluster group ID is set to 20 and session pickup is enabled. Load balance all and the load balancing schedule are set to the default value. The device priority of the primary unit is set to 200. The device priorities of the subordinate units are set to 128 and 100. The host name of the primary unit is `5001_Slot_5`. The host names of the subordinate units are `5001_Slot_3` and `5001_Slot_4`.

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:200 5001_Slot_5 FG50012206400112 0
Slave :100 5001_Slot_3 FG50012205400050 1
Slave :128 5001_Slot_4 FG50012204400045 2
number of vcluster: 1
```

```
vcluster 1: work 169.254.0.1
Master:0 FG50012206400112
Slave :1 FG50012204400045
Slave :2 FG50012205400050
```

The following example shows `get system ha status` output for a cluster of two FortiGate-5001 units with virtual clustering enabled. This command output was produced by logging into the primary unit for virtual cluster 1 (hostname: 5001_Slot_4, serial number FG50012204400045).

The virtual clustering output shows that the cluster unit with host name 5001_Slot_4 and serial number FG50012204400045 is operating as the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2.

For virtual cluster 1 the cluster unit that you have logged into is operating in the work state and the serial number of the primary unit for virtual cluster 1 is FG50012204400045. For virtual cluster 2 the cluster unit that you have logged into is operating in the standby state and the serial number of the primary unit for virtual cluster 2 is FG50012205400050.

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4 FG50012204400045 1
Slave :100 5001_Slot_3 FG50012205400050 0
number of vcluster: 2
vcluster 1: work 169.254.0.2
Master:0 FG50012204400045
Slave :1 FG50012205400050
vcluster 2: standby 169.254.0.1
Slave :1 FG50012204400045
Master:0 FG50012205400050
```

The following example shows `get system ha status` output for the same cluster as shown in the previous example after using `execute ha manage 0` to log into the primary unit for virtual cluster 2 (hostname: 5001_Slot_3, serial number FG50012205400050).

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Slave :100 5001_Slot_3 FG50012205400050 0
Master:128 5001_Slot_4 FG50012204400045 1
number of vcluster: 2
vcluster 1: standby 169.254.0.2
Slave :1 FG50012205400050
Master:0 FG50012204400045
vcluster 2: work 169.254.0.1
Master:0 FG50012205400050
Slave :1 FG50012204400045
```

The following example shows `get system ha status` output for a virtual cluster configuration where the cluster unit with hostname: 5001_Slot_4 and serial number FG50012204400045 is the primary unit for both

virtual clusters. This command output is produced by logging into cluster unit with host name 5001_Slot_4 and serial number FG50012204400045.

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4 FG50012204400045 1
Slave :100 5001_Slot_3 FG50012205400050 0
number of vcluster: 2
vcluster 1: work 169.254.0.2
Master:0 FG50012204400045
Slave :1 FG50012205400050
vcluster 2: work 169.254.0.2
Master:0 FG50012204400045
Slave :1 FG50012205400050
```

About the HA cluster index and the execute ha manage command

When a cluster starts up, the FortiGate Cluster Protocol (FGCP) assigns a cluster index and a HA heartbeat IP address to each cluster unit based on the serial number of the cluster unit. The FGCP selects the cluster unit with the highest serial number to become the primary unit. The FGCP assigns a cluster index of 0 and an HA heartbeat IP address of 169.254.0.1 to this unit. The FGCP assigns a cluster index of 1 and an HA heartbeat IP address of 169.254.0.2 to the cluster unit with the second highest serial number. If the cluster contains more units, the cluster unit with the third highest serial number is assigned a cluster index of 2 and an HA heartbeat IP address of 169.254.0.3, and so on. You can display the cluster index assigned to each cluster unit using the `get system ha status` command. Also when you use the `execute ha manage` command you select a cluster unit to log into by entering its cluster index.

The cluster index and HA heartbeat IP address only change if a unit leaves the cluster or if a new unit joins the cluster. When one of these events happens, the FGCP resets the cluster index and HA heartbeat IP address of each cluster unit according to serial number in the same way as when the cluster first starts up.

Each cluster unit keeps its assigned cluster index and HA heartbeat IP address even as the units take on different roles in the cluster. After the initial cluster index and HA heartbeat IP addresses are set according to serial number, the FGCP checks other primary unit selection criteria such as device priority and monitored interfaces. Checking these criteria could result in selecting a cluster unit without the highest serial number to operate as the primary unit.

Even if the cluster unit without the highest serial number now becomes the primary unit, the cluster indexes and HA heartbeat IP addresses assigned to the individual cluster units do not change. Instead the FGCP assigns a second cluster index, which could be called the operating cluster index, to reflect this role change. The operating cluster index is 0 for the primary unit and 1 and higher for the other units in the cluster. By default both sets of cluster indexes are the same. But if primary unit selection selects the cluster unit that does not have the highest serial number to be the primary unit then this cluster unit is assigned an operating cluster index of 0. The operating cluster index is used by the FGCP only. You can display the operating cluster index assigned to each cluster unit using the `get system ha status` command. There are no CLI commands that reference the operating cluster index.

Even though there are two cluster indexes there is only one HA heartbeat IP address and the HA heartbeat address is not affected by a change in the operating cluster index.

Using the execute ha manage command

When you use the CLI command `execute ha manage <index_integer>` to connect to the CLI of another cluster unit, the `<index_integer>` that you enter is the cluster index of the unit that you want to connect to.

Using get system ha status to display cluster indexes

You can display the cluster index assigned to each cluster unit using the CLI command `get system ha status`. The following example shows the information displayed by the `get system ha status` command for a cluster consisting of two FortiGate-5001SX units operating in active-passive HA mode with virtual domains not enabled and without virtual clustering.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :128 5001_slot_11 FG50012204400045 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG50012205400050
Slave :1 FG50012204400045
```

In this example, the cluster unit with serial number FG50012205400050 has the highest serial number and so has a cluster index of 0 and the cluster unit with serial number FG50012204400045 has a cluster index of 1. From the CLI of the primary (or master) unit of this cluster you can connect to the CLI of the subordinate (or slave) unit using the following command:

```
execute ha manage 1
```

This works because the cluster unit with serial number FG50012204400045 has a cluster index of 1.

The `get system ha status` command output shows two similar lists of indexes and serial numbers. The listing on the sixth and seventh lines of the command output are the cluster indexes assigned according to cluster unit serial number. These are the cluster indexes that you enter when using the `execute ha manage` command. The cluster indexes shown in the last two lines of the command output are the operating cluster indexes that reflect how the cluster units are actually operating in the cluster. In this example both sets of cluster indexes are the same.

The last three lines of the command output display the status of vcluster 1. In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the `get system ha status` command output when you add virtual domains to virtual cluster 2.

The HA heartbeat IP address displayed on line 8 is the HA heartbeat IP address of the cluster unit that is actually operating as the primary unit. For a default configuration this IP address will always be 169.254.0.1 because the cluster unit with the highest serial number will be the primary unit. This IP address changes if the operating primary unit is not the primary unit with the highest serial number.

Example actual and operating cluster indexes do not match

This example shows get system ha status command output for same cluster of two FortiGate-5001SX units. However, in this example the device priority of the cluster unit with the serial number FG50012204400045 is increased to 200. As a result the cluster unit with the lowest serial number becomes the primary unit. This means the actual and operating cluster indexes of the cluster units do not match.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :200 5001_slot_11 FG50012204400045 1
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:1 FG50012205400050
Slave :0 FG50012204400045
```

The actual cluster indexes have not changed but the operating cluster indexes have. Also, the HA heartbeat IP address displayed for vcluster 1 has changed to 169.254.0.2.

Virtual clustering example output

The `get system ha status` command output is the same if a cluster is operating with virtual clustering turned on but with all virtual domains in virtual cluster 1. The following `get system ha status` command output example shows the same cluster operating as a virtual cluster with virtual domains in virtual cluster 1 and added to virtual cluster 2. In this example the cluster unit with serial number FG50012204400045 is the primary unit for virtual cluster 1 and the cluster unit with serial number FG50012205400050 is the primary unit for virtual cluster 2.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :200 5001_slot_11 FG50012204400045 1
number of vcluster: 2
vcluster 1: work 169.254.0.2
Master:1 FG50012205400050
Slave :0 FG50012204400045
vcluster 2: standby 169.254.0.1
Master:0 FG50012205400050
Slave :1 FG50012204400045
```

This example shows three sets of indexes. The indexes in lines six and seven are still used by the `execute ha manage` command. The indexes on lines ten and eleven are for the primary and subordinate units in virtual cluster 1 and the indexes on the last two lines are for virtual cluster 2.

Managing individual cluster units

The following procedure describes how to use SSH to log into the primary unit CLI and from there to use the `execute ha manage` command to connect to the CLI of any other unit in the cluster. The procedure is very similar if you use telnet, or the web-based manager dashboard CLI console.

You can use the `execute ha manage` command from the CLI of any cluster unit to log into the CLI of another the cluster unit. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

Using SSH or telnet or the web-based manager dashboard CLI console you can only log into the primary unit CLI. Using a direct console connection you can log into any cluster unit. In both cases you can use `execute ha manage` to connect to the CLI of other cluster units.

1. Use SSH to connect to the cluster and log into the primary unit CLI.
   Connect to any cluster interface configured for SSH administrative access to log into the cluster.
2. Enter the following command followed by a space and type a question mark (`?`):
   ```
   execute ha manage
   ```
   The CLI displays a list of all the subordinate units in the cluster. Each cluster unit is numbered, starting at 1. The information displayed for each cluster unit includes the unit serial number and the host name of the unit.
3. Complete the command with the number of the subordinate unit to log into. For example, to log into subordinate unit 1, enter the following command:
   ```
   execute ha manage 1
   ```
   Press Enter to connect to and use an administrator account to log into the CLI of the selected subordinate unit. If this subordinate unit has a different host name, the CLI prompt changes to this host name.

   You can use CLI commands to manage this subordinate unit. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.
4. You can now use the `execute ha manage` command to connect to any other cluster unit (including the primary unit). You can also use the `exit` command to return to the primary unit CLI.

Disconnecting a cluster unit from a cluster

Use the following procedures to disconnect a cluster unit from a functioning cluster without disrupting the operation of the cluster. You can disconnect a cluster unit if you need to use the disconnected FortiGate unit for another purpose, such as to act as a standalone firewall.

You can use the following procedures for a standard cluster and for a virtual clustering configuration. To use the following procedures from a virtual cluster you must be logged in as the admin administrator and you must have selected Global Configuration.

When you disconnect a cluster unit you must assign an IP address and netmask to one of the interfaces of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected, the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

When the cluster unit is disconnected the HA mode is changed to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0 except for the interface that you configure.

Otherwise the configuration of the disconnected unit is not changed. The HA configuration of the disconnected unit is not changed either (except to change the HA mode to Standalone).

To disconnect a cluster unit from a cluster - web-based manager

1. Go to **System > Config > HA** to view the cluster members list.
2. Select the Disconnect from cluster icon for the cluster unit to disconnect from the cluster.
3. Select the interface that you want to configure. You also specify the IP address and netmask for this interface. When the FortiGate unit is disconnected, all management access options are enabled for this interface.
4. Specify an IP address and netmask for the interface. You can use this IP address to connect to the interface to configure the disconnected FortiGate unit.
5. Select **OK**.

   The FortiGate unit is disconnected from the cluster and the cluster may renegotiate and select a new primary unit. The selected interface of the disconnected unit is configured with the specified IP address and netmask.

To disconnect a cluster unit from a cluster - CLI

1. Enter the following command to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
execute ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```

Adding a disconnected FortiGate unit back to its cluster

If you disconnect a FortiGate unit from a cluster, you can re-connect the disconnected FortiGate unit to the cluster by setting the HA mode of the disconnected unit to match the HA mode of the cluster. Usually the disconnected unit rejoins the cluster as a subordinate unit and the cluster automatically synchronizes its configuration.

You do not have to change the HA password on the disconnected unit unless the HA password has been changed after the unit was disconnected. Disconnecting a unit from a cluster does not change the HA password.

You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit. You should also make sure that the HA `override` CLI option is not enabled on the disconnected unit. Otherwise, when the disconnected unit joins the cluster, the cluster will renegotiate and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units. This configuration change might disrupt the operation of the cluster.

The following procedure assumes that the disconnected FortiGate unit is correctly physically connected to your network and to the cluster but is not running in HA mode and not part of the cluster.

Before you start this procedure you should note the device priority of the primary unit.

To add a disconnected FortiGate unit back to its cluster - web-based manager

1. Log into the disconnected FortiGate unit.
   If virtual domains are enabled, log in as the admin administrator and select Global Configuration.
2. Go to **System > Config > HA**.
3. Change Mode to match the mode of the cluster.
4. If required, change the group name and password to match the cluster.
5. Set the Device Priority lower than the device priority of the primary unit.
6. Select **OK**.
   The disconnected FortiGate unit joins the cluster.

To add a disconnected FortiGate unit back to its cluster - CLI

1. Log into the CLI of the FortiGate unit to be added back to the cluster.
2. Enter the following command to access the global configuration and add the FortiGate unit back to a cluster operating in active-passive mode and set the device priority to 50 (a low number) so that this unit will not become the primary unit:

```
config global
   config system ha
      set mode a-p
      set priority 50
   end
end
```

   You may have to also change the group name, group id and password. However if you have not changed these for the cluster or the FortiGate unit after it was disconnected from the cluster you should not have to adjust them now.

HA diagnose commands

You can use the following diagnose command to display a data about a cluster:

```
diagnose sys ha dump-by {all-xdb | all-vcluster| rcache | all-group |
   memory | debug-zone | vdom | kernel | device | stat| sesync}
```

The example out put below is from a cluster of two FortiGate-5001Cs. In this cluster the base1 and base2 interfaces communicate the HA heartbeat and port monitoring has been added to poort1.

all-xdb

This command displays information about the current configuration of the cluster and how its operating. You can use the out to determine the primary unit, the state of port monitoring as well as most cluster configuration details and status.

```
diagnose sys ha dump-by all-xdb
HA information.
idx=1,nxentry=2,linkfails=7,flags=0,digest=7.72.e3.2e.8e.d1...
xentry FG-5KC3E13800046 nhbdev=2,nventry=0, hops=0.
base1, 50, mac=0.9.f,bc.e.6c, neighbor=1.
id=FG-5KC3E13800084, mac=0.9.f,bc.11.18.
base2, 50, mac=0.9.f,bc.e.71, neighbor=1.
id=FG-5KC3E13800084, mac=0.9.f,bc.11.1d.
```

```
xentry FG-5KC3E13800084 nhbdev=2,nventry=1, hops=1.
base1, 50, mac=0.9.f,bc.11.18, neighbor=1.
id=FG-5KC3E13800046, mac=0.9.f,bc.e.6c.
base2, 50, mac=0.9.f,bc.11.1d, neighbor=1.
id=FG-5KC3E13800046, mac=0.9.f,bc.e.71.
npath=1,FG-5KC3E13800084
ventry idx=0,id=1,FG-5KC3E13800084,prio=128,0,claimed=0,override=0,flag=0,time=12974,mon=0
mondev=port1,50

idx=0,nxentry=2,linkfails=7,flags=3,digest=7.95.b.9.a8.5d...
xentry FG-5KC3E13800084 nhbdev=2,nventry=1, hops=0.
base1, 50, mac=0.9.f,bc.11.18, neighbor=1.
id=FG-5KC3E13800046, mac=0.9.f,bc.e.6c.
base2, 50, mac=0.9.f,bc.11.1d, neighbor=1.
id=FG-5KC3E13800046, mac=0.9.f,bc.e.71.
ventry idx=0,id=1,FG-5KC3E13800084,prio=128,0,claimed=0,override=0,flag=0,time=12974,mon=0
mondev=port1,50

xentry FG-5KC3E13800046 nhbdev=2,nventry=1, hops=1.
base1, 50, mac=0.9.f,bc.e.6c, neighbor=1.
id=FG-5KC3E13800084, mac=0.9.f,bc.11.18.
base2, 50, mac=0.9.f,bc.e.71, neighbor=1.
id=FG-5KC3E13800084, mac=0.9.f,bc.11.1d.
npath=1,FG-5KC3E13800046
ventry idx=0,id=1,FG-5KC3E13800046,prio=128,0,claimed=0,override=0,flag=0,time=2,mon=0
mondev=port1,50
```

all-vcluster

This command displays the status and configuration of the individual cluster units. You can use the output of this command to determine the primary unit and the status of each cluster unit.

```
diagnose sys ha dump-by all-vcluster
HA information.
vcluster id=1, nventry=2, state=work, digest=5.f8.d1.63.4d.d2...
ventry idx=0,id=1,FG-5KC3E13800046,prio=128,0,claimed=0,override=0,flag=1,time=0,mon=0
mondev=port1,50
ventry idx=1,id=1,FG-5KC3E13800084,prio=128,0,claimed=0,override=0,flag=0,time=12974,mon=0
```

stat

This command displays some statistics about how well the cluster is functioning. Information includes packet counts, memory use, failed links and ping failures.

```
diagnose sys ha dump-by stat
HA information.
packet count = 1, memory = 220.
check_linkfails = 0, linkfails = 0, check_pingsvrfails = 2822
bufcnt = -5, bufmem = 0
```

HA and failover protection

In FortiGate active-passive HA, the FortiGate Clustering Protocol (FGCP) provides failover protection. This means that an active-passive cluster can provide FortiGate services even when one of the cluster units encounters a problem that would result in complete loss of connectivity for a stand-aloneFortiGate unit. This failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially in a mission-critical environment.

The FGCP supports three kinds of failover protection. Device failover automatically replaces a failed device and restarts traffic flow with minimal impact on the network. Link failover maintains traffic flow if a link fails. Session failover resumes communication sessions with minimal loss of data if a device or link failover occurs.

This chapter describes how FGCP failover protection works and provides detailed NAT/Route and Transparent mode packet flow descriptions.

About active-passive failover

To achieve failover protection in an active-passive cluster, one of the cluster units functions as the primary unit, while the rest of the cluster units are subordinate units, operating in an active stand-by mode. The cluster IP addresses and HA virtual MAC addresses are associated with the cluster interfaces of the primary unit. All traffic directed at the cluster is actually sent to and processed by the primary unit.

While the cluster is functioning, the primary unit functions as the FortiGate network security device for the networks that it is connected to. In addition, the primary unit and subordinate units use the HA heartbeat to keep in constant communication. The subordinate units report their status to the cluster unit and receive and store connection and state table updates.

Device failure

If the primary unit encounters a problem that is severe enough to cause it to fail, the remaining cluster units negotiate to select a new primary unit. This occurs because all of the subordinate units are constantly waiting to negotiate to become primary units. Only the heartbeat packets sent by the primary unit keep the subordinate units from becoming primary units. Each received heartbeat packet resets negotiation timers in the subordinate units. If this timer is allowed to run out because the subordinate units do not receive heartbeat packets from the primary unit, the subordinate units assume that the primary unit has failed, and negotiate to become primary units themselves.

Using the same FGCP negotiation process that occurs when the cluster starts up, after they determine that the primary unit has failed, the subordinate units negotiate amongst themselves to select a new primary unit. The subordinate unit that wins the negotiation becomes the new primary unit with the same MAC and IP addresses as the former primary unit. The new primary unit then sends gratuitous ARP packets out all of its interfaces to inform attached switches to send traffic to the new primary unit. Sessions then resume with the new primary unit.

Link failure

If a primary unit interface fails or is disconnected while a cluster is operation, a link failure occurs. When a link failure occurs the cluster units negotiate to select a new primary unit. Since the primary unit has not stopped operating, it participates in the negotiation. The link failure means that a new primary unit must be selected and the cluster unit with the link failure joins the cluster as a subordinate unit.

Just as for a device failover, the new primary unit sends gratuitous arp packets out all of its interfaces to inform attached switches to send traffic to it. Sessions then resume with the new primary unit.

If a subordinate unit experiences a device failure its status in the cluster does not change. However, in future negotiations a cluster unit with a link failure is unlikely to become the primary unit.

Session failover

If you enable session failover (also called session pickup) for the cluster, during cluster operation the primary unit informs the subordinate units of changes to the primary unit connection and state tables, keeping the subordinate units up-to-date with the traffic currently being processed by the cluster.

After a failover the new primary unit recognizes open sessions that were being handled by the cluster. The sessions continue to be processed by the new primary unit and are handled according to their last known state.

If you leave session pickup disabled, the cluster does not keep track of sessions and after a failover, active sessions have to be restarted or resumed.

Primary unit recovery

If a primary unit recovers after a device or link failure, it will operate as a subordinate unit, unless the `override` CLI keyword is enabled and its device priority is set higher than the unit priority of other cluster units (see HA override).

About active-active failover

HA failover in a cluster running in active-active mode is similar to active-passive failover described above. Active-active subordinate units are constantly waiting to negotiate to become primary units and, if session failover is enabled, continuously receive connection state information from the primary unit. If the primary unit fails, or one of the primary unit interfaces fails, the cluster units use the same mechanisms to detect the failure and to negotiate to select a new primary unit. If session failover is enabled, the new primary unit also maintains communication sessions through the cluster using the shared connection state table.

Active-active HA load balances sessions among all cluster units. For session failover, the cluster must maintain all of these sessions. To load balance sessions, the functioning cluster uses a load balancing schedule to distribute sessions to all cluster units. The shared connection state table tracks the communication sessions being processed by all cluster units (not just the primary unit). After a failover, the new primary unit uses the load balancing schedule to re-distribute all of the communication sessions recorded in the shared connection state table among all of the remaining cluster units. The connections continue to be processed by the cluster, but possibly by a different cluster unit, and are handled according to their last known state.

Device failover

The FGCP provides transparent device failover. Device failover is a basic requirement of any highly available system. Device failover means that if a device fails, a replacement device automatically takes the place of the failed device and continues operating in the same manner as the failed device.

In the case of FortiOS HA, the device is the primary unit. If the primary unit fails, device failover ensures that one of the subordinate units in the cluster automatically takes the place of the primary unit and can continue processing network traffic in the same way as the failed primary unit.

Device failover does not maintain communication sessions. After a device failover, communication sessions have to be restarted. To maintain communication sessions, you must enable session failover. See Session failover (session pick-up) on page 1496.

FortiGate HA device failover is supported by the HA heartbeat, virtual MAC addresses, configuration synchronization, route synchronization and IPsec VPN SA synchronization.

The HA heartbeat makes sure that the subordinate units detect a primary unit failure. If the primary unit fails to respond on time to HA heartbeat packets the subordinate units assume that the primary unit has failed and negotiate to select a new primary unit.

The new primary unit takes the place of the failed primary unit and continues functioning in the same way as the failed primary unit. For the new primary unit to continue functioning like the failed primary unit, the new primary unit must be able to reconnect to network devices and the new primary unit must have the same configuration as the failed primary unit.

FortiGate HA uses virtual MAC addresses to reconnect the new primary unit to network devices. The FGCP causes the new primary unit interfaces to acquire the same virtual MAC addresses as the failed primary unit. As a result, the new primary unit has the same network identity as the failed primary unit.

The new primary unit interfaces have different physical connections than the failed primary unit. Both the failed and the new primary unit interfaces are connected to the same switches, but the new primary unit interfaces are connected to different ports on these switches. To make sure that the switches send packets to the new primary unit, the new primary unit interfaces send gratuitous ARP packets to the connected switches. These gratuitous ARP packets notify the switches that the primary unit MAC and IP addresses are on different switch ports and cause the switches to send packets to the ports connected to the new primary unit. In this way, the new primary unit continues to receive packets that would otherwise have been sent to the failed primary unit.

Configuration synchronization means that the new primary unit always has the same configuration as the failed primary unit. As a result the new primary unit operates in exactly the same way as the failed primary unit. If configuration synchronization were not available the new primary unit may not process network traffic in the same way as the failed primary unit.

Kernel routing table synchronization synchronizes the primary unit kernel routing table to all subordinate units so that after a failover the new primary unit does not have to form a completely new routing table. IPsec VPN SA synchronization synchronizes IPsec VPN security associations (SAs) and other IPsec session data so that after a failover the new primary unit can resume IPsec tunnels without having to establish new SAs.

HA heartbeat and communication between cluster units

The HA heartbeat keeps cluster units communicating with each other. The heartbeat consists of hello packets that are sent at regular intervals by the heartbeat interface of all cluster units. These hello packets describe the state of the cluster unit and are used by other cluster units to keep all cluster units synchronized.

HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. The default time interval between HA heartbeats is 200 ms. The FGCP uses link-local IP4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

For best results, isolate the heartbeat devices from your user networks by connecting the heartbeat devices to a separate switch that is not connected to any network. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a crossover cable. Heartbeat packets contain sensitive

information about the cluster configuration. Heartbeat packets may also use a considerable amount of network bandwidth. For these reasons, it is preferable to isolate heartbeat packets from your user networks.

On startup, a FortiGate unit configured for HA operation broadcasts HA heartbeat hello packets from its HA heartbeat interface to find other FortiGate units configured to operate in HA mode. If two or more FortiGate units operating in HA mode connect with each other, they compare HA configurations (HA mode, HA password, and HA group ID). If the HA configurations match, the units negotiate to form a cluster.

While the cluster is operating, the HA heartbeat confirms that all cluster units are functioning normally. The heartbeat also reports the state of all cluster units, including the communication sessions that they are processing.

Heartbeat interfaces

A heartbeat interface is an Ethernet network interface in a cluster that is used by the FGCP for HA heartbeat communications between cluster units.

To change the HA heartbeat configuration go to **System > Config > HA** and select the *FortiGate interfaces* to use as HA heartbeat interfaces.

Do not use a switch port for the HA heartbeat traffic. This configuration is not supported.

From the CLI enter the following command to make port4 and port5 HA heartbeat interfaces and give both interfaces a heartbeat priority of 150:

```
config system ha
   set hbdev port4 150 port5 150
end
```

The following example shows how to change the default heartbeat interface configuration so that the port4 and port1 interfaces can be used for HA heartbeat communication and to give the port4 interface the highest heartbeat priority so that port4 is the preferred HA heartbeat interface.

```
config system ha
   set hbdev port4 100 port1 50
end
```

By default, for most FortiGate models two interfaces are configured to be heartbeat interfaces. You can change the heartbeat interface configuration as required. For example you can select additional or different heartbeat interfaces. You can also select only one heartbeat interface.

In addition to selecting the heartbeat interfaces, you also set the **Priority** for each heartbeat interface. In all cases, the heartbeat interface with the highest priority is used for all HA heartbeat communication. If the interface fails or becomes disconnected, the selected heartbeat interface that has the next highest priority handles all heartbeat communication.

If more than one heartbeat interface has the same priority, the heartbeat interface with the highest priority that is also highest in the heartbeat interface list is used for all HA heartbeat communication. If this interface fails or becomes disconnected, the selected heartbeat interface with the highest priority that is next highest in the list handles all heartbeat communication.

The default heartbeat interface configuration sets the priority of two heartbeat interfaces to 50. You can accept the default heartbeat interface configuration if one or both of the default heartbeat interfaces are connected. You can select different heartbeat interfaces, select more heartbeat interfaces and change heartbeat priorities according to your requirements.

For the HA cluster to function correctly, you must select at least one heartbeat interface and this interface of all of the cluster units must be connected together. If heartbeat communication is interrupted and cannot failover to a second heartbeat interface, the cluster units will not be able to communicate with each other and more than one cluster unit may become a primary unit. As a result the cluster stops functioning normally because multiple devices on the network may be operating as primary units with the same IP and MAC addresses creating a kind if split brain scenario.

The heartbeat interface priority range is 0 to 512. The default priority when you select a new heartbeat interface is 0. The higher the number the higher the priority.

In most cases you can maintain the default heartbeat interface configuration as long as you can connect the heartbeat interfaces together. Configuring HA heartbeat interfaces is the same for virtual clustering and for standard HA clustering.

You can enable heartbeat communications for physical interfaces, but not for VLAN subinterfaces, IPsec VPN interfaces, redundant interfaces, or for 802.3ad aggregate interfaces. You cannot select these types of interfaces in the heartbeat interface list.

Selecting more heartbeat interfaces increases reliability. If a heartbeat interface fails or is disconnected, the HA heartbeat fails over to the next heartbeat interface.

You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces.

HA heartbeat traffic can use a considerable amount of network bandwidth. If possible, enable HA heartbeat traffic on interfaces used only for HA heartbeat traffic or on interfaces connected to less busy networks.

Connecting HA heartbeat interfaces

For most FortiGate models if you do not change the heartbeat interface configuration, you can isolate the default heartbeat interfaces of all of the cluster units by connecting them all to the same switch. Use one switch per heartbeat interface. If the cluster consists of two units you can connect the heartbeat interfaces together using crossover cables.

HA heartbeat and data traffic are supported on the same cluster interface. In NAT/Route mode, if you decide to use heartbeat interfaces for processing network traffic or for a management connection, you can assign the interface any IP address. This IP address does not affect HA heartbeat traffic.

In Transparent mode, you can connect the heartbeat interface to your network and enable management access. You would then establish a management connection to the interface using the Transparent mode management IP address. This configuration does not affect HA heartbeat traffic.

Heartbeat packets and heartbeat interface selection

HA heartbeat hello packets are constantly sent by all of the enabled heartbeat interfaces. Using these hello packets, each cluster unit confirms that the other cluster units are still operating. The FGCP selects one of the heartbeat interfaces to be used for communication between the cluster units. The FGCP selects the heartbeat interface for heartbeat communication based on the linkfail states of the heartbeat interfaces, on the priority of the heartbeat interfaces, and on the interface index.

The FGCP checks the linkfail state of all heartbeat interfaces to determine which ones are connected. The FGCP selects one of these connected heartbeat interfaces to be the one used for heartbeat communication. The FGCP selects the connected heartbeat interface with the highest priority for heartbeat communication.

If more than one connected heartbeat interface has the highest priority the FGCP selects the heartbeat interface with the lowest interface index. The web-based manager lists the FortiGate unit interfaces in alphabetical order. This order corresponds to the interface index order with lowest index at the top and highest at the bottom. If more than one heartbeat interface has the highest priority, the FGCP selects the interface that is highest in the heartbeat interface list (or first in alphabetical order) for heartbeat communication.

If the interface that is processing heartbeat traffic fails or becomes disconnected, the FGCP uses the same criteria to select another heartbeat interface for heartbeat communication. If the original heartbeat interface is fixed or reconnected, the FGCP again selects this interface for heartbeat communication.

The HA heartbeat communicates cluster session information, synchronizes the cluster configuration, synchronizes the cluster kernel routing table, and reports individual cluster member status. The HA heartbeat constantly communicates HA status information to make sure that the cluster is operating properly.

Interface index and display order

The web-based manager and CLI display interface names in alphanumeric order. For example, the sort order for a FortiGate unit with 10 interfaces (named port1 through port10) places port10 at the bottom of the list:

- port1
- port2 through 9
- port10

However, interfaces are indexed in hash map order, rather than purely by alphabetic order or purely by interface number value comparisons. As a result, the list is sorted primarily alphabetical by interface name (for example, base1 is before port1), then secondarily by index numbers:

- port1
- port10
- port2 through port9

HA heartbeat interface IP addresses

The FGCP uses link-local IP4 addresses (RFC 3927) in the 169.254.0.x range for HA heartbeat interface IP addresses and for inter-VDOM link interface IP addresses. When a cluster initially starts up, the primary unit heartbeat interface IP address is 169.254.0.1. Subordinate units are assigned heartbeat interface IP addresses in the range 169.254.0.2 to 169.254.0.63. HA inter-VDOM link interfaces on the primary unit are assigned IP addresses 169.254.0.65 and 169.254.0.66.

The ninth line of the following CLI command output shows the HA heartbeat interface IP address of the primary unit.

```
get system ha status
   Model: 620
   Mode: a-p
   Group: 0
   Debug: 0
   ses_pickup: disable
   Master:150 head_office_upper FG600B3908600825 1
   Slave :150 head_office_lower FG600B3908600705 0
   number of vcluster: 1
   vcluster 1: work 169.254.0.1
   Master:0 FG600B3908600825
   Slave :1 FG600B3908600705
```

You can also use the `execute traceroute` command from the subordinate unit CLI to display HA heartbeat IP addresses and the HA inter-VDOM link IP addresses. For example, use `execute ha manage 1` to connect to the subordinate unit CLI and then enter the following command to trace the route to an IP address on your network:

```
execute traceroute 172.20.20.10
   traceroute to 172.20.20.10 (172.20.20.10), 32 hops max, 72 byte packets
       1 169.254.0.1 0 ms 0 ms 0 ms
       2 169.254.0.66 0 ms 0 ms 0 ms
       3 172.20.20.10 0 ms 0 ms 0 ms
```

Both HA heartbeat and data traffic are supported on the same FortiGate interface. All heartbeat communication takes place on a separate VDOM called vsys_ha. Heartbeat traffic uses a virtual interface called port_ha in the vsys_ha VDOM. Data and heartbeat traffic use the same physical interface, but they're logically separated into separate VDOMs.

Heartbeat packet Ethertypes

Normal IP packets are 802.3 packets that have an Ethernet type (Ethertype) field value of 0x0800. Ethertype values other than 0x0800 are understood as level2 frames rather than IP packets.

By default, HA heartbeat packets use the following Ethertypes:

- HA heartbeat packets for NAT/Route mode clusters use Ethertype 0x8890. These packets are used by cluster units to find other cluster units and to verify the status of other cluster units while the cluster is operating. You can change the Ethertype of these packets using the `ha-eth-type` option of the `config system ha` command.
- HA heartbeat packets for Transparent mode clusters use Ethertype 0x8891. These packets are used by cluster units to find other cluster units and to verify the status of other cluster units while the cluster is operating. You can change the Ethertype of these packets using the `hc-eth-type` option of the `config system ha` command.
- HA telnet sessions between cluster units over HA heartbeat links use Ethertype 0x8893. The telnet sessions are used to synchronize the cluster configurations. Telnet sessions are also used when an administrator uses the `execute ha manage` command to connect from one cluster unit CLI to another. You can change the Ethertype of these packets using the `l2ep-eth-type` option of the `config system ha` command.

Because heartbeat packets are recognized as level2 frames, the switches and routers on your heartbeat network that connect to heartbeat interfaces must be configured to allow them. If level2 frames are dropped by these network devices, heartbeat traffic will not be allowed between the cluster units.

Some third-party network equipment may use packets with these Ethertypes for other purposes. For example, Cisco N5K/Nexus switches use Ethertype 0x8890 for some functions. When one of these switches receives Ethertype 0x8890 packets from an attached cluster unit, the switch generates CRC errors and the packets are not forwarded. As a result, FortiGate units connected with these switches cannot form a cluster.

In some cases, if the heartbeat interfaces are connected and configured so regular traffic flows but heartbeat traffic is not forwarded, you can change the configuration of the switch that connects the HA heartbeat interfaces to allow level2 frames with Ethertypes 0x8890, 0x8893, and 0x8891 to pass.

Alternatively, you can use the following CLI options to change the Ethertypes of the HA heartbeat packets:

```
config system ha
   set ha-eth-type <ha_ethertype_4-digit_hex
   set hc-eth-type <hc_ethertype_4-digit_ex>
   set l2ep-eth-type <l2ep_ethertype_4-digit_hex>
end
```

For example, use the following command to change the Ethertype of the HA heartbeat packets from 0x8890 to 0x8895 and to change the Ethertype of HA Telnet session packets from 0x8891 to 0x889f:

```
config system ha
   set ha-eth-type 8895
   set l2ep-eth-type 889f
end
```

Modifying heartbeat timing

In an HA cluster, if a cluster unit CPU becomes very busy, the cluster unit may not be able to send heartbeat packets on time. If heartbeat packets are not sent on time other units in the cluster may think that the cluster unit has failed and the cluster will experience a failover.

A cluster unit CPU may become very busy if the cluster is subject to a syn flood attack, if network traffic is very heavy, or for other similar reasons. You can use the following CLI commands to configure how the cluster times HA heartbeat packets:

```
config system ha
   set hb-interval <interval_integer>
   set hb-lost-threshold <threshold_integer>
   set helo-holddown <holddown_integer>
end
```

Changing the lost heartbeat threshold

The lost heartbeat threshold is the number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The default value is 6, meaning that if the 6 heartbeat packets are not received from a cluster unit then that cluster unit is considered to have failed. The range is 1 to 60 packets.

If the primary unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The lower the `hb-lost-threshold` the faster a cluster responds when a unit fails. However, sometimes heartbeat packets may not be sent because a cluster unit is very busy. This can lead to a false positive failure detection. To reduce these false positives you can increase the `hb-lost-threshold`.

Use the following CLI command to increase the lost heartbeat threshold to 12:

```
config system ha
   set hb-lost-threshold 12
end
```

Changing the heartbeat interval

The heartbeat interval is the time between sending HA heartbeat packets. The heartbeat interval range is 1 to 20 (100*ms). The heartbeat interval default is 2 (200 ms).

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms (5 * 100ms = 500ms).

The HA heartbeat packets consume more bandwidth if the heartbeat interval is short. But if the heartbeat interval is very long, the cluster is not as sensitive to topology and other network changes.

Use the following CLI command to increase the heartbeat interval to 10:

```
config system ha
   set hb-interval 10
end
```

The heartbeat interval combines with the lost heartbeat threshold to set how long a cluster unit waits before assuming that another cluster unit has failed and is no longer sending heartbeat packets. By default, if a cluster unit does not receive a heartbeat packet from a cluster unit for 6 * 200 = 1200 milliseconds or 1.2 seconds the cluster unit assumes that the other cluster unit has failed.

You can increase both the heartbeat interval and the lost heartbeat threshold to reduce false positives. For example, increasing the heartbeat interval to 20 and the lost heartbeat threshold to 30 means a failure will be assumed if no heartbeat packets are received after 30 * 2000 milliseconds = 60,000 milliseconds, or 60 seconds.

Use the following CLI command to increase the heartbeat interval to 20 and the lost heartbeat threshold to 30:

```
config system ha
   set hb-lost-threshold 20
   set hb-interval 30
end
```

Changing the time to wait in the helo state

The hello state hold-down time is the number of seconds that a cluster unit waits before changing from hello state to work state. After a failure or when starting up, cluster units operate in the hello state to send and receive heartbeat packets so that all the cluster units can find each other and form a cluster. A cluster unit should change from the hello state to work state after it finds all of the other FortiGate units to form a cluster with. If for some reason all cluster units cannot find each other during the hello state then some cluster units may be joining the cluster after it has formed. This can cause disruptions to the cluster and affect how it operates.

One reason for a delay in all of the cluster units joining the cluster could be the cluster units are located at different sites of if for some other reason communication is delayed between the heartbeat interfaces.

If cluster units are joining your cluster after it has started up of if it takes a while for units to join the cluster you can increase the time that the cluster units wait in the helo state. The hello state hold-down time range is 5 to 300 seconds. The hello state hold-down time default is 20 seconds.

Use the following CLI command to increase the time to wait in the helo state to 1 minute (60 seconds):

```
config system ha
   set helo-holddown 60
end
```

Enabling or disabling HA heartbeat encryption and authentication

You can enable HA heartbeat encryption and authentication to encrypt and authenticate HA heartbeat packets. HA heartbeat packets should be encrypted and authenticated if the cluster interfaces that send HA heartbeat packets are also connected to your networks.

If HA heartbeat packets are not encrypted the cluster password and changes to the cluster configuration could be exposed and an attacker may be able to sniff HA packets to get cluster information. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.

HA heartbeat encryption and authentication are disabled by default. Enabling HA encryption and authentication could reduce cluster performance. Use the following CLI command to enable HA heartbeat encryption and authentication.

```
config system ha
```

```
    set authentication enable
    set encryption enable
end
```

HA authentication and encryption uses AES-128 for encryption and SHA1 for authentication.

Cluster virtual MAC addresses

When a cluster is operating, the FGCP assigns virtual MAC addresses to each primary unit interface. HA uses virtual MAC addresses so that if a failover occurs, the new primary unit interfaces will have the same virtual MAC addresses and IP addresses as the failed primary unit. As a result, most network equipment would identify the new primary unit as the exact same device as the failed primary unit.

If the MAC addresses changed after a failover, the network would take longer to recover because all attached network devices would have to learn the new MAC addresses before they could communicate with the cluster.

If a cluster is operating in NAT/Route mode, the FGCP assigns a different virtual MAC address to each primary unit interface. VLAN subinterfaces are assigned the same virtual MAC address as the physical interface that the VLAN subinterface is added to. Redundant interfaces or 802.3ad aggregate interfaces are assigned the virtual MAC address of the first interface in the redundant or aggregate list.

If a cluster is operating in Transparent mode, the FGCP assigns a virtual MAC address for the primary unit management IP address. Since you can connect to the management IP address from any interface, all of the FortiGate interfaces appear to have the same virtual MAC address.

A MAC address conflict can occur if two clusters are operating on the same network. See Diagnosing packet loss with two FortiGate HA clusters in the same broadcast domain on page 1469 for more information.

Subordinate unit MAC addresses do not change. You can verify this by connecting to the subordinate unit CLI and using the `get hardware interface nic` command to display the MAC addresses of each FortiGate interface.

The MAC address of a reserved management interface is not changed to a virtual MAC address. Instead the reserved management interface keeps its original MAC address.

When the new primary unit is selected after a failover, the primary unit sends gratuitous ARP packets to update the devices connected to the cluster interfaces (usually layer-2 switches) with the virtual MAC address. Gratuitous ARP packets configure connected network devices to associate the cluster virtual MAC addresses and cluster IP address with primary unit physical interfaces and with the layer-2 switch physical interfaces. This is sometimes called using gratuitous ARP packets (sometimes called GARP packets) to train the network. The gratuitous ARP packets sent from the primary unit are intended to make sure that the layer-2 switch forwarding databases (FDBs) are updated as quickly as possible.

Sending gratuitous ARP packets is not required for routers and hosts on the network because the new primary unit will have the same MAC and IP addresses as the failed primary unit. However, since the new primary unit interfaces are connected to different switch interfaces than the failed primary unit, many network switches will update their FDBs more quickly after a failover if the new primary unit sends gratuitous ARP packets.

Changing how the primary unit sends gratuitous ARP packets after a failover

When a failover occurs it is important that the devices connected to the primary unit update their FDBs as quickly as possible to reestablish traffic forwarding.

Depending on your network configuration, you may be able to change the number of gratuitous ARP packets and the time interval between ARP packets to reduce the cluster failover time.

You cannot disable sending gratuitous ARP packets, but you can use the following command to change the number of packets that are sent. For example, enter the following command to send 20 gratuitous ARP packets:

```
config system ha
   set arps 20
end
```

You can use this command to configure the primary unit to send from 1 to 60 ARP packets. Usually you would not change the default setting of 5. In some cases, however, you might want to reduce the number of gratuitous ARP packets. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending a higher number gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully, you could reduce the number of gratuitous ARP packets that are sent to reduce the amount of traffic produced after a failover.

If failover is taking longer that expected, you may be able to reduce the failover time by increasing the number gratuitous ARP packets sent.

You can also use the following command to change the time interval in seconds between gratuitous ARP packets. For example, enter the following command to change the time between ARP packets to 3 seconds:

```
config system ha
   set arps-interval 3
end
```

The time interval can be in the range of 1 to 20 seconds. The default is 8 seconds between gratuitous ARP packets. Normally you would not need to change the time interval. However, you could decrease the time to be able send more packets in less time if your cluster takes a long time to failover.

There may also be a number of reasons to set the interval higher. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully you could increase the interval to reduce the amount of traffic produced after a failover.

For more information about gratuitous ARP packets see RFC 826 and RFC 3927.

Disabling gratuitous ARP packets after a failover

You can use the following command to turn off sending gratuitous ARP packets after a failover:

```
config system ha
   set gratuitous-arps disable
end
```

Sending gratuitous ARP packets is turned on by default.

In most cases you would want to send gratuitous ARP packets because its a reliable way for the cluster to notify the network to send traffic to the new primary unit. However, in some cases, sending gratuitous ARP packets may be less optimal. For example, if you have a cluster of FortiGate units in Transparent mode, after a failover the new primary unit will send gratuitous ARP packets to all of the addresses in its Forwarding Database (FDB). If the

FDB has a large number of addresses it may take extra time to send all the packets and the sudden burst of traffic could disrupt the network.

If you choose to disable sending gratuitous ARP packets you must first enable the `link-failed-signal` setting. The cluster must have some way of informing attached network devices that a failover has occurred.

For more information about the `link-failed-signal` setting, see Updating MAC forwarding tables when a link failover occurs on page 1489.

How the virtual MAC address is determined

The virtual MAC address is determined based on following formula:

```
00-09-0f-09-<group-id_hex>-(<vcluster_integer> + <idx>)
```

where

`<group-id_hex>` is the HA Group ID for the cluster converted to hexadecimal.The following table lists the virtual MAC address set for each group ID.

HA group ID in integer and hexadecimal format

Integer Group ID	Hexadecimal Group ID
0	00
1	01
2	02
3	03
4	04
…	…
10	0a
11	0b
…	…
63	3f
…	…
255	ff

`<vcluster_integer>` is 0 for virtual cluster 1 and 20 for virtual cluster 2. If virtual domains are not enabled, HA sets the virtual cluster to 1 and by default all interfaces are in the root virtual domain. Including virtual cluster and virtual domain factors in the virtual MAC address formula means that the same formula can be used whether or not virtual domains and virtual clustering is enabled.

<idx> is the index number of the interface. Interfaces are numbered from 0 to x (where x is the number of interfaces). Interfaces are numbered according to their has map order. See Interface index and display order on page 1460. The first interface has an index of 0. The second interface in the list has an index of 1 and so on.

Only the <idx> part of the virtual MAC address is different for each interface. The <vcluster_integer> would be different for different interfaces if multiple VDOMs have been added.

Between FortiOS releases interface indexing may change so the virtual MAC addresses assigned to individual FortiGate interfaces may also change.

Example virtual MAC addresses

An HA cluster with HA group ID unchanged (default=0) and virtual domains not enabled would have the following virtual MAC addresses for interfaces port1 to port12:

- port1 virtual MAC: 00-09-0f-09-00-00
- port10 virtual MAC: 00-09-0f-09-00-01
- port2 virtual MAC: 00-09-0f-09-00-02
- port3 virtual MAC: 00-09-0f-09-00-03
- port4 virtual MAC: 00-09-0f-09-00-04
- port5 virtual MAC: 00-09-0f-09-00-05
- port6 virtual MAC: 00-09-0f-09-00-06
- port7 virtual MAC: 00-09-0f-09-00-07
- port8 virtual MAC: 00-09-0f-09-00-08
- port9 virtual MAC: 00-09-0f-09-00-09
- port11 virtual MAC: 00-09-0f-09-00-0a
- port12 virtual MAC: 00-09-0f-09-00-0b

If the group ID is changed to 34 these virtual MAC addresses change to:

- port1 virtual MAC: 00-09-0f-09-22-00
- port3 virtual MAC: 00-09-0f-09-22-03
- port4 virtual MAC: 00-09-0f-09-22-04
- port5 virtual MAC: 00-09-0f-09-22-05
- port6 virtual MAC: 00-09-0f-09-22-06
- port7 virtual MAC: 00-09-0f-09-22-07
- port8 virtual MAC: 00-09-0f-09-22-08
- port9 virtual MAC: 00-09-0f-09-22-09
- port11 virtual MAC: 00-09-0f-09-22-0a
- port12 virtual MAC: 00-09-0f-09-22-0b
- port10 virtual MAC: 00-09-0f-09-22-01
- port2 virtual MAC: 00-09-0f-09-22-02

A cluster with virtual domains enabled where the HA group ID has been changed to 23, port5 and port 6 are in the root virtual domain (which is in virtual cluster1), and port7 and port8 are in the vdom_1 virtual domain (which is in virtual cluster 2) would have the following virtual MAC addresses:

- port5 interface virtual MAC: `00-09-0f-09-23-05`
- port6 interface virtual MAC: `00-09-0f-09-23-06`
- port7 interface virtual MAC: `00-09-0f-09-23-27`
- port8 interface virtual MAC: `00-09-0f-09-23-28`

Displaying the virtual MAC address

Every FortiGate unit physical interface has two MAC addresses: the current hardware address and the permanent hardware address. The permanent hardware address cannot be changed, it is the actual MAC address of the interface hardware. The current hardware address can be changed. The current hardware address is the address seen by the network. For a FortiGate unit not operating in HA, you can use the following command to change the current hardware address of the port1 interface:

```
config system interface
   edit port1
      set macaddr <mac_address>
   end
end
```

For an operating cluster, the current hardware address of each cluster unit interface is changed to the HA virtual MAC address by the FGCP. The `macaddr` option is not available for a functioning cluster. You cannot change an interface MAC address and you cannot view MAC addresses from the `system interface` CLI command.

You can use the `get hardware nic <interface_name_str>` command to display both MAC addresses for any FortiGate interface. This command displays hardware information for the specified interface. Depending on their hardware configuration, this command may display different information for different interfaces. You can use this command to display the current hardware address as `Current_HWaddr` and the permanent hardware address as `Permanent_HWaddr`. For some interfaces the current hardware address is displayed as `MAC`. The command displays a great deal of information about the interface so you may have to scroll the output to find the hardware addresses.

You can also use the `diagnose hardware deviceinfo nic <interface_str>` command to display both MAC addresses for any FortiGate interface.

Before HA configuration the current and permanent hardware addresses are the same. For example for one of the units in Cluster_1:

```
FGT60B3907503171 # get hardware nic internal
.
.
.
MAC: 02:09:0f:78:18:c9
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

During HA operation the current hardware address becomes the HA virtual MAC address, for example for the units in Cluster_1:

```
FGT60B3907503171 # get hardware nic internal
```

```
.
.
.
MAC: 00:09:0f:09:00:02
Permanent_HWaddr: 02:09:0f:78:18:c9
.
.
.
```

The following command output for Cluster_2 shows the same current hardware address for port1 as for the internal interface of Cluster_2, indicating a MAC address conflict.

```
FG300A2904500238 # get hardware nic port1
.
.
.
MAC: 00:09:0f:09:00:02
Permanent_HWaddr: 00:09:0F:85:40:FD
.
.
.
```

Diagnosing packet loss with two FortiGate HA clusters in the same broadcast domain

A network may experience packet loss when two FortiGate HA clusters have been deployed in the same broadcast domain. Deploying two HA clusters in the same broadcast domain can result in packet loss because of MAC address conflicts. The packet loss can be diagnosed by pinging from one cluster to the other or by pinging both of the clusters from a device within the broadcast domain. You can resolve the MAC address conflict by changing the HA Group ID configuration of the two clusters. The HA Group ID is sometimes also called the Cluster ID.

This section describes a topology that can result in packet loss, how to determine if packets are being lost, and how to correct the problem by changing the HA Group ID.

Packet loss on a network can also be caused by IP address conflicts. Finding and fixing IP address conflicts can be difficult. However, if you are experiencing packet loss and your network contains two FortiGate HA clusters you can use the information in this article to eliminate one possible source of packet loss.

Changing the HA group ID to avoid MAC address conflicts

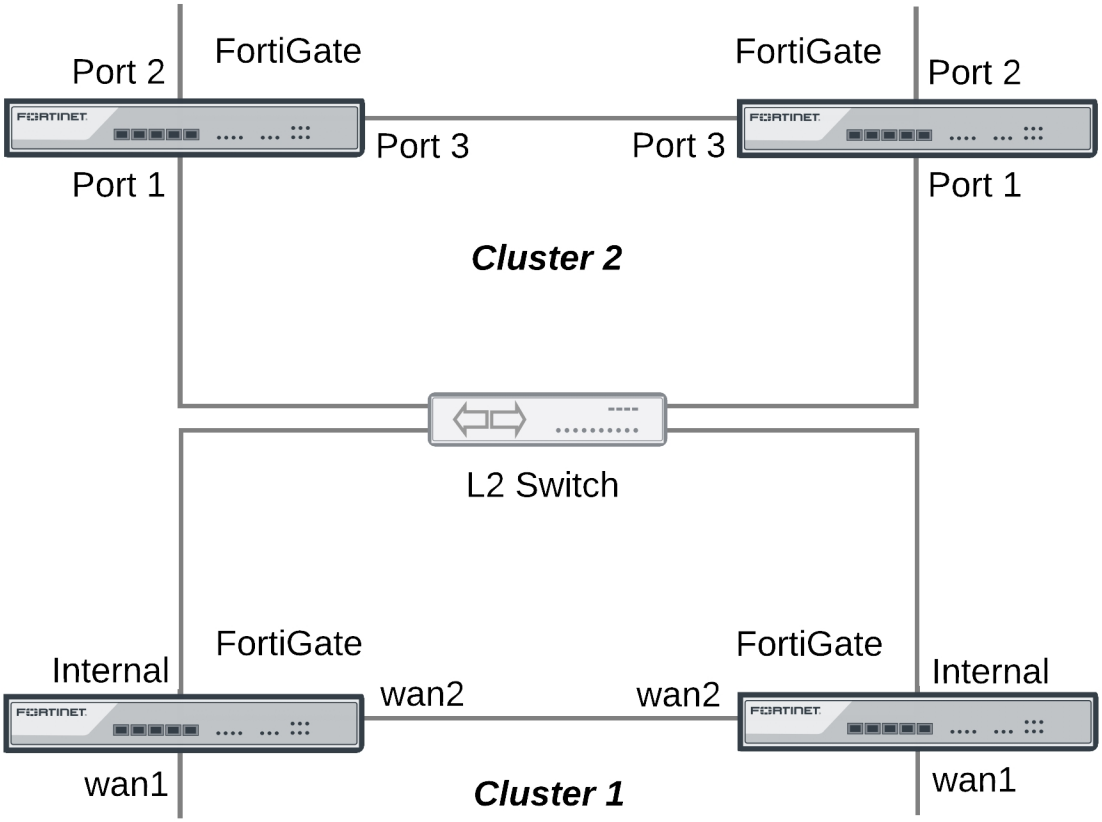
Change the Group ID to change the virtual MAC address of all cluster interfaces. You can change the Group ID from the FortiGate CLI using the following command:

```
config system ha
   set group-id <id_integer>
end
```

Example topology

The topology below shows two clusters. The Cluster_1 internal interfaces and the Cluster_2 port 1 interfaces are both connected to the same broadcast domain. In this topology the broadcast domain could be an internal network. Both clusters could also be connected to the Internet or to different networks.

Example HA topology with possible MAC address conflicts



Ping testing for packet loss

If the network is experiencing packet loss, it is possible that you will not notice a problem unless you are constantly pinging both HA clusters. During normal operation of the network you also might not notice packet loss because the loss rate may not be severe enough to timeout TCP sessions. Also many common types if TCP traffic, such as web browsing, may not be greatly affected by packet loss. However, packet loss can have a significant effect on real time protocols that deliver audio and video data.

To test for packet loss you can set up two constant ping sessions, one to each cluster. If packet loss is occurring the two ping sessions should show alternating replies and timeouts from each cluster.

Cluster_1	Cluster_2
reply	timeout
reply	timeout
reply	timeout
timeout	reply
timeout	reply
reply	timeout
reply	timeout
timeout	reply
timeout	reply
timeout	reply
timeout	reply

Viewing MAC address conflicts on attached switches

If two HA clusters with the same virtual MAC address are connected to the same broadcast domain (L2 switch or hub), the MAC address will conflict and bounce between the two clusters. This example Cisco switch MAC address table shows the MAC address flapping between different interfaces (1/0/1 and 1/0/4).

```
1 0009.0f09.0002 DYNAMIC Gi1/0/1
1 0009.0f09.0002 DYNAMIC Gi1/0/4
```

Synchronizing the configuration

The FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit.

The following settings are not synchronized between cluster units:

- HA override.
- HA device priority.
- The virtual cluster priority.
- The FortiGate unit host name.
- The HA priority setting for a ping server (or dead gateway detection) configuration.
- The system interface settings of the HA reserved management interface.
- The HA default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command.

The primary unit synchronizes all other configuration settings, including the other HA configuration settings.

Disabling automatic configuration synchronization

In some cases you may want to use the following command to disable automatic synchronization of the primary unit configuration to all cluster units.

```
config system ha
   set sync-config disable
end
```

When this option is disabled the cluster no longer synchronizes configuration changes. If a device failure occurs, the new primary unit may not have the same configuration as the failed primary unit. As a result, the new primary unit may process sessions differently or may not function on the network in the same way.

In most cases you should not disable automatic configuration synchronization. However, if you have disabled this feature you can use the `execute ha synchronize` command to manually synchronize a subordinate unit's configuration to that of the primary unit.

You must enter `execute ha synchronize` commands from the subordinate unit that you want to synchronize with the primary unit. Use the `execute ha manage` command to access a subordinate unit CLI.

For example, to access the first subordinate unit and force a synchronization at any time, even if automatic synchronization is disabled enter:

```
execute ha manage 0
execute ha synchronize start
```

You can use the following command to stop a synchronization that is in progress.

```
execute ha synchronize stop
```

Incremental synchronization

When you log into the cluster web-based manager or CLI to make configuration changes, you are actually logging into the primary unit. All of your configuration changes are first made to the primary unit. Incremental synchronization then immediately synchronizes these changes to all of the subordinate units.

When you log into a subordinate unit CLI (for example using `execute ha manage`) all of the configuration changes that you make to the subordinate unit are also immediately synchronized to all cluster units, including the primary unit, using the same process.

Incremental synchronization also synchronizes other dynamic configuration information such as the DHCP server address lease database, routing table updates, IPsec SAs, MAC address tables, and so on. SeeAn introduction to the FGCP on page 1270 for more information about DHCP server address lease synchronization and Synchronizing kernel routing tables on page 1480 for information about routing table updates.

Whenever a change is made to a cluster unit configuration, incremental synchronization sends the same configuration change to all other cluster units over the HA heartbeat link. An HA synchronization process running on the each cluster unit receives the configuration change and applies it to the cluster unit. The HA synchronization process makes the configuration change by entering a CLI command that appears to be entered by the administrator who made the configuration change in the first place.

Synchronization takes place silently, and no log messages are recorded about the synchronization activity. However, log messages can be recorded by the cluster units when the synchronization process enters CLI commands. You can see these log messages on the subordinate units if you enable event logging and set the minimum severity level to **Information** and then check the event log messages written by the cluster units when you make a configuration change.

You can also see these log messages on the primary unit if you make configuration changes from a subordinate unit.

Periodic synchronization

Incremental synchronization makes sure that as an administrator makes configuration changes, the configurations of all cluster units remain the same. However, a number of factors could cause one or more cluster units to go out of sync with the primary unit. For example, if you add a new unit to a functioning cluster, the configuration of this new unit will not match the configuration of the other cluster units. Its not practical to use incremental synchronization to change the configuration of the new unit.

Periodic synchronization is a mechanism that looks for synchronization problems and fixes them. Every minute the cluster compares the configuration file checksum of the primary unit with the configuration file checksums of each of the subordinate units. If all subordinate unit checksums are the same as the primary unit checksum, all cluster units are considered synchronized.

If one or more of the subordinate unit checksums is not the same as the primary unit checksum, the subordinate unit configuration is considered out of sync with the primary unit. The checksum of the out of sync subordinate unit is checked again every 15 seconds. This re-checking occurs in case the configurations are out of sync because an incremental configuration sequence has not completed. If the checksums do not match after 5 checks the subordinate unit that is out of sync retrieves the configuration from the primary unit. The subordinate unit then reloads its configuration and resumes operating as a subordinate unit with the same configuration as the primary unit.

The configuration of the subordinate unit is reset in this way because when a subordinate unit configuration gets out of sync with the primary unit configuration there is no efficient way to determine what the configuration differences are and to correct them. Resetting the subordinate unit configuration becomes the most efficient way to resynchronize the subordinate unit.

Synchronization requires that all cluster units run the same FortiOS firmware build. If some cluster units are running different firmware builds, then unstable cluster operation may occur and the cluster units may not be able to synchronize correctly.

Re-installing the firmware build running on the primary unit forces the primary unit to upgrade all cluster units to the same firmware build.

Console messages when configuration synchronization succeeds

When a cluster first forms, or when a new unit is added to a cluster as a subordinate unit, the following messages appear on the CLI console to indicate that the unit joined the cluster and had its configuring synchronized with the primary unit.

```
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
   slave's configuration is not in sync with master's, sequence:2
   slave's configuration is not in sync with master's, sequence:3
   slave's configuration is not in sync with master's, sequence:4
   slave starts to sync with master
logout all admin users
slave succeeded to sync with master
```

Console messages when configuration synchronization fails

If you connect to the console of a subordinate unit that is out of synchronization with the primary unit, messages similar to the following are displayed.

```
slave is not in sync with master, sequence:0. (type 0x3)
slave is not in sync with master, sequence:1. (type 0x3)
slave is not in sync with master, sequence:2. (type 0x3)
slave is not in sync with master, sequence:3. (type 0x3)
slave is not in sync with master, sequence:4. (type 0x3)
global compared not matched
```

If synchronization problems occur the console message sequence may be repeated over and over again. The messages all include a type value (in the example `type 0x3`). The type value can help Fortinet Support diagnose the synchronization problem.

HA out of sync object messages and the configuration objects that they reference

Out of Sync Message	Configuration Object
HA_SYNC_SETTING_CONFIGURATION = 0x03	/data/config
HA_SYNC_SETTING_AV = 0x10	
HA_SYNC_SETTING_VIR_DB = 0x11	/etc/vir
HA_SYNC_SETTING_SHARED_LIB = 0x12	/data/lib/libav.so
HA_SYNC_SETTING_SCAN_UNIT = 0x13	/bin/scanunitd
HA_SYNC_SETTING_IMAP_PRXY = 0x14	/bin/imapd
HA_SYNC_SETTING_SMTP_PRXY = 0x15	/bin/smtp
HA_SYNC_SETTING_POP3_PRXY = 0x16	/bin/pop3
HA_SYNC_SETTING_HTTP_PRXY = 0x17	/bin/thttp
HA_SYNC_SETTING_FTP_PRXY = 0x18	/bin/ftpd
HA_SYNC_SETTING_FCNI = 0x19	/etc/fcni.dat
HA_SYNC_SETTING_FDNI = 0x1a	/etc/fdnservers.dat
HA_SYNC_SETTING_FSCI = 0x1b	/etc/sci.dat
HA_SYNC_SETTING_FSAE = 0x1c	/etc/fsae_adgrp.cache
HA_SYNC_SETTING_IDS = 0x20	/etc/ids.rules
HA_SYNC_SETTING_IDSUSER_RULES = 0x21	/etc/idsuser.rules
HA_SYNC_SETTING_IDSCUSTOM = 0x22	
HA_SYNC_SETTING_IDS_MONITOR = 0x23	/bin/ipsmonitor
HA_SYNC_SETTING_IDS_SENSOR = 0x24	/bin/ipsengine
HA_SYNC_SETTING_NIDS_LIB = 0x25	/data/lib/libips.so
HA_SYNC_SETTING_WEBLISTS = 0x30	
HA_SYNC_SETTING_CONTENTFILTER = 0x31	/data/cmdb/webfilter.bword
HA_SYNC_SETTING_URLFILTER = 0x32	/data/cmdb/webfilter.urlfilter
HA_SYNC_SETTING_FTGD_OVRD = 0x33	/data/cmdb/webfilter.fgtd-ovrd

Out of Sync Message	Configuration Object
HA_SYNC_SETTING_FTGD_LRATING = 0x34	/data/cmdb/webfilter.fgtd-ovrd
HA_SYNC_SETTING_EMAILLISTS = 0x40	
HA_SYNC_SETTING_EMAILCONTENT = 0x41	/data/cmdb/spamfilter.bword
HA_SYNC_SETTING_EMAILBWLIST = 0x42	/data/cmdb/spamfilter.emailbwl
HA_SYNC_SETTING_IPBWL = 0x43	/data/cmdb/spamfilter.ipbwl
HA_SYNC_SETTING_MHEADER = 0x44	/data/cmdb/spamfilter.mheader
HA_SYNC_SETTING_RBL = 0x45	/data/cmdb/spamfilter.rbl
HA_SYNC_SETTING_CERT_CONF = 0x50	/etc/cert/cert.conf
HA_SYNC_SETTING_CERT_CA = 0x51	/etc/cert/ca
HA_SYNC_SETTING_CERT_LOCAL = 0x52	/etc/cert/local
HA_SYNC_SETTING_CERT_CRL = 0x53	/etc/cert/crl
HA_SYNC_SETTING_DB_VER = 0x55	
HA_GET_DETAIL_CSUM = 0x71	
HA_SYNC_CC_SIG = 0x75	/etc/cc_sig.dat
HA_SYNC_CC_OP = 0x76	/etc/cc_op
HA_SYNC_CC_MAIN = 0x77	/etc/cc_main
HA_SYNC_FTGD_CAT_LIST = 0x7a	/migadmin/webfilter/ublock/ftgd/data/

Comparing checksums of cluster units

You can use the `diagnose sys ha showcsum` command to compare the configuration checksums of all cluster units. The output of this command shows checksums labelled `global` and `all` as well as checksums for each of the VDOMs including the `root` VDOM. The `get system ha-nonsync-csum` command can be used to display similar information; however, this command is intended to be used by FortiManager.

The primary unit and subordinate unit checksums should be the same. If they are not you can use the `execute ha synchronize` command to force a synchronization.

The following command output is for the primary unit of a cluster that does not have multiple VDOMs enabled:

```
diagnose sys ha showcsum
is_manage_master()=1, is_root_master()=1
debugzone
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
```

```
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5

checksum
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5
```

The following command output is for a subordinate unit of the same cluster:

```
diagnose sys ha showcsum
is_manage_master()=0, is_root_master()=0
debugzone
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5

checksum
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5
```

The following example shows using this command for the primary unit of a cluster with multiple VDOMs. Two VDOMs have been added named `test` and `Eng_vdm`.

From the primary unit:

```
config global
   sys ha showcsum
   is_manage_master()=1, is_root_master()=1
   debugzone
   global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
   test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
   root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
   Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
   all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53

   checksum
   global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
   test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
   root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
   Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
   all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53
```

From the subordinate unit:

```
config global
   diagnose sys ha showcsum
   is_manage_master()=0, is_root_master()=0
   debugzone
   global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
   test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
   root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
   Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
   all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53

   checksum
   global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
   test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
   root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
   Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
```

```
all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53
```

How to diagnose HA out of sync messages

This section describes how to use the commands `diagnose sys ha showcsum` and `diagnose debug` to diagnose the cause of HA out of sync messages.

If HA synchronization is not successful, use the following procedures on each cluster unit to find the cause.

To determine why HA synchronization does not occur

1. Connect to each cluster unit CLI by connected to the console port.
2. Enter the following commands to enable debugging and display HA out of sync messages.

   ```
   diagnose debug enable
   diagnose debug console timestamp enable
   diagnose debug application hatalk -1
   diagnose debug application hasync -1
   ```

   Collect the console output and compare the out of sync messages with the information on page 203.
3. Enter the following commands to turn off debugging.

   ```
   diagnose debug disable
   diagnose debug reset
   ```

To determine what part of the configuration is causing the problem

If the previous procedure displays messages that include sync object 0x30 (for example, `HA_SYNC_SETTING_CONFIGURATION = 0x03`) there is a synchronization problem with the configuration. Use the following steps to determine the part of the configuration that is causing the problem.

If your cluster consists of two cluster units, use this procedure to capture the configuration checksums for each unit. If your cluster consists of more that two cluster units, repeat this procedure for all cluster units that returned messages that include 0x30 sync object messages.

1. Connect to each cluster unit CLI by connected to the console port.
2. Enter the following command to turn on terminal capture

   ```
   diagnose debug enable
   ```
3. Enter the following command to stop HA synchronization.

   ```
   execute ha sync stop
   ```
4. Enter the following command to display configuration checksums.

   ```
   diagnose sys ha showcsum 1
   ```
5. Copy the output to a text file.
6. Repeat for all affected units.
7. Compare the text file from the primary unit with the text file from each cluster unit to find the checksums that do not match.

   You can use a diff function to compare text files.
8. Repeat steps 4 to 7 for each checksum level:

   ```
   diagnose sys ha showcsum 2
   diagnose sys ha showcsum 3
   diagnose sys ha showcsum 4
   diagnose sys ha showcsum 5
   ```

```
diagnose sys ha showcsum 6
diagnose sys ha showcsum 7
diagnose sys ha showcsum 8
```

9. When the non-matching checksum is found, attempt to drill down further. This is possible for objects that have sub-components.

   For example you can enter the following commands:

   ```
   diagnose sys ha showcsum system.global
   diagnose sys ha showcsum system.interface
   ```

   Generally it is the first non-matching checksum in one of the levels that is the cause of the synchronization problem.

10. Attempt to can remove/change the part of the configuration that is causing the problem. You can do this by making configuration changes from the primary unit or subordinate unit CLI.
11. Enter the following commands to start HA configuration and stop debugging:

    ```
    execute ha sync start
    diagnose debug disable
    diagnose debug reset
    ```

Recalculating the checksums to resolve out of sync messages

Sometimes an error can occur when checksums are being calculated by the cluster. As a result of this calculation error the CLI console could display out of sync error messages even though the cluster is otherwise operating normally. You can also sometimes see checksum calculation errors in `diagnose sys ha showcsum` command output when the checksums listed in the `debugzone` output don't match the checksums in the `checksum` part of the output.

One solution to this problem could be to re-calculate the checksums. The re-calculated checksums should match and the out of sync error messages should stop appearing.

You can use the following command to re-calculate HA checksums:

```
diagnose sys ha csum-recalculate [<vdom-name> | global]
```

Just entering the command without options recalculates all checksums. You can specify a VDOM name to just recalculate the checksums for that VDOM. You can also enter `global` to recalculate the global checksum.

Synchronizing kernel routing tables

In a functioning cluster, the primary unit keeps all subordinate unit kernel routing tables (also called the forwarding information base FIB) up to date and synchronized with the primary unit. After a failover, because of these routing table updates the new primary unit does not have to populate its kernel routing table before being able to route traffic. This gives the new primary unit time to rebuild its regular routing table after a failover.

Use the following command to view the regular routing table. This table contains all of the configured routes and routes acquired from dynamic routing protocols and so on. This routing table is not synchronized. On subordinate units this command will not produce the same output as on the primary unit.

```
get router info routing-table
```

Use the following command to view the kernel routing table (FIB). This is the list of resolved routes actually being used by the FortiOS kernel. The output of this command should be the same on the primary unit and the subordinate units.

```
get router info kernel
```

This section describes how clusters handle dynamic routing failover and also describes how to use CLI commands to control the timing of routing table updates of the subordinate unit routing tables from the primary unit.

Controlling how the FGCP synchronizes kernel routing table updates

You can use the following commands to control some of the timing settings that the FGCP uses when synchronizing routing updates from the primary unit to subordinate units and maintaining routes on the primary unit after a failover.

```
config system ha
   set route-hold <hold_integer>
   set route-ttl <ttl_integer>
   set route-wait <wait_integer>
end
```

Change how long routes stay in a cluster unit routing table

Change the `route-ttl` time to control how long routes remain in a cluster unit routing table. The time to live range is 5 to 3600 seconds. The default time to live is 10 seconds.

The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes.

By default, `route-ttl` is set to 10 which may mean that only a few routes will remain in the routing table after a failover. Normally keeping `route-ttl` to 10 or reducing the value to 5 is acceptable because acquiring new routes usually occurs very quickly, especially if graceful restart is enabled, so only a minor delay is caused by acquiring new routes.

If the primary unit needs to acquire a very large number of routes, or if for other reasons, there is a delay in acquiring all routes, the primary unit may not be able to maintain all communication sessions.

You can increase the route time to live if you find that communication sessions are lost after a failover so that the primary unit can use synchronized routes that are already in the routing table, instead of waiting to acquire new routes.

Change the time between routing updates

Change the `route-hold` time to change the time that the primary unit waits between sending routing table updates to subordinate units. The route hold range is 0 to 3600 seconds. The default route hold time is 10 seconds.

To avoid flooding routing table updates to subordinate units, set `route-hold` to a relatively long time to prevent subsequent updates from occurring too quickly. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Increasing the time between updates means that this data exchange will not have to happen so often.

The `route-hold` time should be coordinated with the `route-wait` time.

Change the time the primary unit waits after receiving a routing update

Change the `route-wait` time to change how long the primary unit waits after receiving routing updates before sending the updates to the subordinate units. For quick routing table updates to occur, set route-wait to a

relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units.

The `route-wait` range is 0 to 3600 seconds. The default `route-wait` is 0 seconds.

Normally, because the `route-wait` time is 0 seconds the primary unit sends routing table updates to the subordinate units every time its routing table changes.

Once a routing table update is sent, the primary unit waits the `route-hold` time before sending the next update.

Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so `route-wait` is set to 0 seconds. `route-hold` can be set to a relatively long time because normally the next route update would not occur for a while.

In some cases, routing table updates can occur in bursts. A large burst of routing table updates can occur if a router or a link on a network fails or changes. When a burst of routing table updates occurs, there is a potential that the primary unit could flood the subordinate units with routing table updates. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Setting `route-wait` to a longer time reduces the frequency of additional updates are and prevents flooding of routing table updates from occurring.

Configuring graceful restart for dynamic routing failover

When an HA failover occurs, neighbor routers will detect that the cluster has failed and remove it from the network until the routing topology stabilizes. During that time the routers may stop sending IP packets to the cluster and communication sessions that would normally be processed by the cluster may time out or be dropped. Also the new primary unit will not receive routing updates and so will not be able to build and maintain its routing database.

You can solve this problem by configuring graceful restart for the dynamic routing protocols that you are using. This section describes configuring graceful restart for OSPF and BGP.

To support graceful restart you should make sure the new primary unit keeps its synchronized routing data long enough to acquire new routing data. You should also increase the HA route time to live, route wait, and route hold values to 60 using the following CLI command:

```
config system ha
   set route-ttl 60
   set route-wait 60
   set route-hold 60
end
```

Graceful OSPF restart

You can configure graceful restart (also called nonstop forwarding (NSF)) as described in RFC3623 (Graceful OSPF Restart) to solve the problem of dynamic routing failover. If graceful restart is enabled on neighbor routers, they will keep sending packets to the cluster following the HA failover instead of removing it from the network. The neighboring routers assume that the cluster is experiencing a graceful restart.

After the failover, the new primary unit can continue to process communication sessions using the synchronized routing data received from the failed primary unit before the failover. This gives the new primary unit time to update its routing table after the failover.

You can use the following commands to enable graceful restart or NSF on Cisco routers:

```
router ospf 1
```

```
    log-adjacency-changes
    nsf ietf helper strict-lsa-checking
```

If the cluster is running OSPF, use the following command to enable graceful restart for OSFP:

```
config router ospf
   set restart-mode graceful-restart
end
```

Graceful BGP restart

If the cluster is running BGP only the primary unit keeps BGP peering connections. When a failover occurs, the BGP peering needs to be reestablished. This will happen if you enable BGP graceful restart which causes the adjacent routers to keep the routes active while the BGP peering is restarted by the new primary unit.

> Enabling BGP graceful restart causes the FortiGate's BGP process to restart which can temporarily disrupt traffic through the cluster. So normally you should wait for a quiet time or a maintenance period to enable BGP graceful restart.

Use the following command to enable graceful restart for BGP and set some graceful restart options.

```
config router bgp
   set graceful-restart enable
   set graceful-restart-time 120
   set graceful-stalepath-time 360
   set graceful-update-delay 120
end
```

Notifing BGP neighbors when graceful restart is enabled

You can add BGP neighbors and configure the cluster unit to notify these neighbors that it supports graceful restart.

```
config router bgp
   config neighbor
      edit <neighbor_address_Ipv4>
         set capability-graceful-restart enable
      end
end
```

Bidirectional Forwarding Detection (BFD) enabled BGP graceful restart

You can add a BFD enabled BGP neighbor as a static BFD neighbor using the following command. This example shows how to add a BFD neighbor with IP address 172.20.121.23 that is on the network connected to port4:

```
config router bfd
   config neighbor
      edit 172.20.121.23
         set port4
      end
   end
```

The FGCP supports graceful restart of BFD enabled BGP neighbors. The `config router bfd` command is needed as the BGP auto-start timer is 5 seconds. After HA failover, BGP on the new primary unit has to wait for 5 seconds to connect to its neighbors, and then register BFD requests after establishing the connections. With static BFD neighbors, BFD requests and sessions can be created as soon as possible after the failover. The new command `get router info bfd requests` shows the BFD peer requests.

A BFD session created for a static BFD neighbor/peer request will initialize its state as "INIT" instead of "DOWN" and its detection time `asbfd-required-min-rx * bfd-detect-mult` milliseconds.

When a BFD control packet with nonzero your_discr is received, if no session can be found to match the your_discr, instead of discarding the packet, other fields in the packet, such as addressing information, are used to choose one session that was just initialized, with zero as its remote discriminator.

When a BFD session in the up state receives a control packet with zero as your_discr and down as the state, the session will change its state into down but will not notify this down event to BGP and/or other registered clients.

Synchronizing IPsec VPN SAs

The FGCP synchronizes IPsec security associations (SAs) between cluster members so that if a failover occurs, the cluster can resume IPsec sessions without having to establish new SAs. The result is improved failover performance because IPsec sessions are not interrupted to establish new SAs. Also, establishing a large number of SAs can reduce cluster performance.

The FGCP implements slightly different synchronization mechanisms for IKEv1 and IKEv2.

Synchronizing SAs for IKEv1

When an SA is synchronized to the subordinate units. the sequence number is set to the maximum sequence number. After a failover, all inbound traffic that connects with the new primary unit and uses the SA will be accepted without needing to re-key. However, first outbound packet to use the SA causes the sequence number to overflow and so causes the new primary unit to re-key the SA.

Please note the following:

- The cluster synchronizes all IPsec SAs.
- IPsec SAs are not synchronized until the IKE process has finished synchronizing the ISAKMP SAs. This is required in for dialup tunnels since it is the synchronizing of the ISAKMP SA that creates the dialup tunnel.
- A dialup interface is created as soon as the phase1 is complete. This ensures that the when HA synchronizes phase1 information the dialup name is included.
- If the IKE process re-starts for any reason it deletes any dialup tunnels that exist. This forces the peer to re-key them.
- IPsec SA deletion happens immediately. Routes associated with a dialup tunnel that is being deleted are cleaned up synchronously as part of the delete, rather than waiting for the SA hard-expiry.
- The FGCP does not sync the IPsec tunnel MTU from the primary unit to the subordinate units. This means that after HA failover if the first packet received by the FortiGate unit arrives after the HA route has been deleted and before the new route is added and the packet is larger than the default MTU of 1024 then the FortiGate unit sends back an ICMP fragmentation required. However, as soon as routing is re-established then the MTU will be corrected and traffic will flow.

Synchronizing SAs for IKEv2

Due to the way the IKEv2 protocol is designed the FGCP cannot use exactly the same solution that is used for synchronizing IKEv1 SAs, though it is similar.

For IKEv2, like IKEv1, the FGCP synchronizes IKE and ISAKMP SAs from the primary unit to the subordinate units. However, for IKEv2 the FGCP cannot actually use this IKE SA to send/receive IKE traffic because IKEv2 includes a sequence number in every IKE message and thus it would require synchronizing every message to the subordinate units to keep the sequence numbers on the subordinate units up to date.

Instead, the FGCP synchronizes IKEv2 Message IDs. This Message ID Sync allows IKEv2 to re-negotiate send and receive message ID counters after a failover. By doing this, the established IKE SA can remain up, instead of re-negotiating.

The `diagnose vpn ike stats` command shows statistics for the number of HA messages sent/received for IKEv2. The output of this command includes a number of fields prefixed with `ha` that contain high availably related-data. For example:

```
.
.
.
ha.resync: 0
ha.vike.sync: 0
ha.conn.sync: 0
ha.sync.tx: 1
ha.sync.rx: 0
ha.sync.rx.len.bad: 0
.
.
.
```

Link failover (port monitoring or interface monitoring)

Link failover means that if a monitored interface fails, the cluster reorganizes to reestablish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic.

You configure monitored interfaces (also called interface monitoring or port monitoring) by selecting the interfaces to monitor as part of the cluster HA configuration.

You can monitor up to 64 interfaces.

The interfaces that you can monitor appear on the port monitor list. You can monitor all FortiGate interfaces including redundant interfaces and 802.3ad aggregate interfaces.

You cannot monitor the following types of interfaces (you cannot select the interfaces on the port monitor list):

- FortiGate interfaces that contain an internal switch.
- VLAN subinterfaces.
- IPsec VPN interfaces.
- Individual physical interfaces that have been added to a redundant or 802.3ad aggregate interface.
- FortiGate-5000 series backplane interfaces that have not been configured as network interfaces.

If you are configuring a virtual cluster you can create a different port monitor configuration for each virtual cluster. Usually for each virtual cluster you would monitor the interfaces that have been added to the virtual domains in each virtual cluster.

Wait until after the cluster is up and running to enable interface monitoring. You do not need to configure interface monitoring to get a cluster up and running and interface monitoring will cause failovers if for some reason during initial setup a monitored interface has become disconnected. You can always enable interface monitoring once you have verified that the cluster is connected and operating properly.

You should only monitor interfaces that are connected to networks, because a failover may occur if you monitor an unconnected interface.

To enable interface monitoring - web-based manager

Use the following steps to monitor the port1 and port2 interfaces of a cluster.

1. Connect to the cluster web-based manager.
2. Go to **System > Config > HA** and edit the primary unit (**Role** is **MASTER**).
3. Select the **Port Monitor** check boxes for the **port1** and **port2** interfaces and select **OK**.
   The configuration change is synchronized to all cluster units.

To enable interface monitoring - CLI

Use the following steps to monitor the port1 and port2 interfaces of a cluster.

1. Connect to the cluster CLI.
2. Enter the following command to enable interface monitoring for port1 and port2.

```
configure system ha
   set monitor port1 port2
end
```

The following example shows how to enable monitoring for the external, internal, and DMZ interfaces.

```
config system ha
   set monitor external internal dmz
end
```

With interface monitoring enabled, during cluster operation, the cluster monitors each cluster unit to determine if the monitored interfaces are operating and connected. Each cluster unit can detect a failure of its network interface hardware. Cluster units can also detect if its network interfaces are disconnected from the switch they should be connected to.

Cluster units cannot determine if the switch that its interfaces are connected to is still connected to the network. However, you can use remote IP monitoring to make sure that the cluster unit can connect to downstream network devices. See Remote link failover on page 1491.

Because the primary unit receives all traffic processed by the cluster, a cluster can only process traffic from a network if the primary unit can connect to it. So, if the link between a network and the primary unit fails, to maintain communication with this network, the cluster must select a different primary unit; one that is still connected to the network. Unless another link failure has occurred, the new primary unit will have an active link to the network and will be able to maintain communication with it.

To support link failover, each cluster unit stores link state information for all monitored cluster units in a link state database. All cluster units keep this link state database up to date by sharing link state information with the other cluster units. If one of the monitored interfaces on one of the cluster units becomes disconnected or fails, this information is immediately shared with all cluster units.

If a monitored interface on the primary unit fails

If a monitored interface on the primary unit fails, the cluster renegotiates to select a new primary unit using the process described in An introduction to the FGCP on page 1270. Because the cluster unit with the failed monitored interface has the lowest monitor priority, a different cluster unit becomes the primary unit. The new primary unit should have fewer link failures.

After the failover, the cluster resumes and maintains communication sessions in the same way as for a device failure. See Device failover on page 1456.

If a monitored interface on a subordinate unit fails

If a monitored interface on a subordinate unit fails, this information is shared with all cluster units. The cluster does not renegotiate. The subordinate unit with the failed monitored interface continues to function in the cluster.

In an active-passive cluster after a subordinate unit link failover, the subordinate unit continues to function normally as a subordinate unit in the cluster.

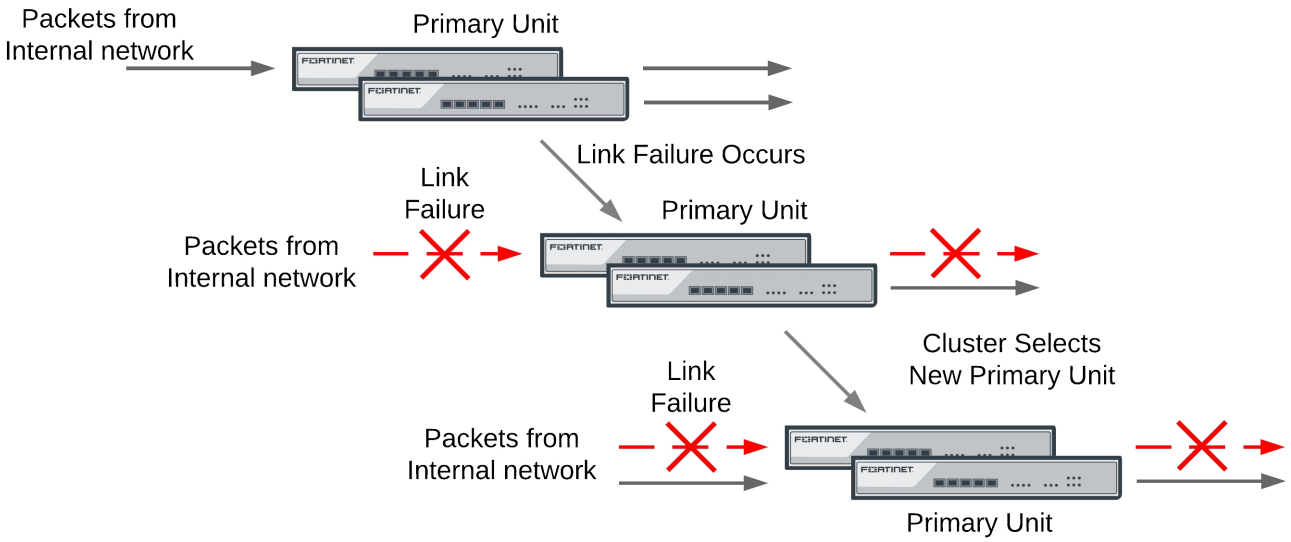
In an active-active cluster after a subordinate unit link failure:

- The subordinate unit with the failed monitored interface can continue processing connections between functioning interfaces. However, the primary unit stops sending sessions to a subordinate unit that use any failed monitored interfaces on the subordinate unit.
- If session pickup is enabled, all sessions being processed by the subordinate unit failed interface that can be failed over are failed over to other cluster units. Sessions that cannot be failed over are lost and have to be restarted.
- If session pickup is not enabled all sessions being processed by the subordinate unit failed interface are lost.

How link failover maintains traffic flow

Monitoring an interface means that the interface is connected to a high priority network. As a high priority network, the cluster should maintain traffic flow to and from the network, even if a link failure occurs. Because the primary unit receives all traffic processed by the cluster, a cluster can only process traffic from a network if the primary unit can connect to it. So, if the link that the primary unit has to a high priority network fails, to maintain traffic flow to and from this network, the cluster must select a different primary unit. This new primary unit should have an active link to the high priority network.

A link failure causes a cluster to select a new primary unit



If a monitored interface on the primary unit fails, the cluster renegotiates and selects the cluster unit with the highest monitor priority to become the new primary unit. The cluster unit with the highest monitor priority is the cluster unit with the most monitored interfaces connected to networks.

After a link failover, the primary unit processes all traffic and all subordinate units, even the cluster unit with the link failure, share session and link status. In addition all configuration changes, routes, and IPsec SAs are synchronized to the cluster unit with the link failure.

In an active-active cluster, the primary unit load balances traffic to all the units in the cluster. The cluster unit with the link failure can process connections between its functioning interfaces (for, example if the cluster has connections to an internal, external, and DMZ network, the cluster unit with the link failure can still process connections between the external and DMZ networks).

Recovery after a link failover and controlling primary unit selection (controlling falling back to the prior primary unit)

If you find and correct the problem that caused a link failure (for example, re-connect a disconnected network cable) the cluster updates its link state database and re-negotiates to select a primary unit.

What happens next depends on how the cluster configuration affects primary unit selection:

- The former primary unit will once again become the primary unit (falling back to becoming the primary unit)
- The primary unit will not change.

As described in An introduction to the FGCP on page 1270, when the link is restored, if no options are configured to control primary unit selection and the cluster age difference is less than 300 seconds the former primary unit will once again become the primary unit. If the age differences are greater than 300 seconds then a new primary unit is not selected. Since you have no control on the age difference the outcome can be unpredictable. This is not a problem in cases where its not important which unit becomes the primary unit.

Preventing a primary unit change after a failed link is restored

Some organizations will not want the cluster to change primary units when the link is restored. Instead they would rather wait to restore the primary unit during a maintenance window. This functionality is not directly supported, but you can experiment with changing some primary unit selection settings. For example, in most cases it should work to enable override on all cluster units and make sure their priorities are the same. This should mean that the primary unit should not change after a failed link is restored.

Then, when you want to restore the original primary unit during a maintenance window you can just set its Device Priority higher. After it becomes the primary unit you can reset all device priorities to the same value. Alternatively during a maintenance window you could reboot the current primary unit and any subordinate units except the one that you want to become the primary unit.

If the `override` CLI keyword is enabled on one or more cluster units and the device priority of a cluster unit is set higher than the others, when the link failure is repaired and the cluster unit with the highest device priority will always become the primary unit.

Testing link failover

You can test link failure by disconnecting the network cable from a monitored interface of a cluster unit. If you disconnect a cable from a primary unit monitored interface the cluster should renegotiate and select one of the other cluster units as the primary unit. You can also verify that traffic received by the disconnected interface continues to be processed by the cluster after the failover.

If you disconnect a cable from a subordinate unit interface the cluster will not renegotiate.

Updating MAC forwarding tables when a link failover occurs

When a FortiGate HA cluster is operating and a monitored interface fails on the primary unit, the primary unit usually becomes a subordinate unit and another cluster unit becomes the primary unit. After a link failover, the new primary unit sends gratuitous ARP packets to refresh the MAC forwarding tables (also called arp tables) of the switches connected to the cluster. This is normal link failover operation.

Even when gratuitous ARP packets are sent, some switches may not be able to detect that the primary unit has become a subordinate unit and will keep sending packets to the former primary unit. This can occur if the switch does not detect the failure and does not clear its MAC forwarding table.

You have another option available to make sure the switch detects the failover and clears its MAC forwarding tables. You can use the following command to cause a cluster unit with a monitored interface link failure to briefly shut down all of its interfaces (except the heartbeat interfaces) after the failover occurs:

```
config system ha
   set link-failed-signal enable
end
```

Usually this means each interface of the former primary unit is shut down for about a second. When this happens the switch should be able to detect this failure and clear its MAC forwarding tables of the MAC addresses of the former primary unit and pickup the MAC addresses of the new primary unit. Each interface will shut down for a

second but the entire process usually takes a few seconds. The more interfaces the FortiGate unit has, the longer it will take.

Normally, the new primary unit also sends gratuitous ARP packets that also help the switch update its MAC forwarding tables to connect to the new primary unit. If `link-failed-signal` is enabled, sending gratuitous ARP packets is optional and can be disabled if you don't need it or if its causing problems. See Disabling gratuitous ARP packets after a failover on page 1465.

Multiple link failures

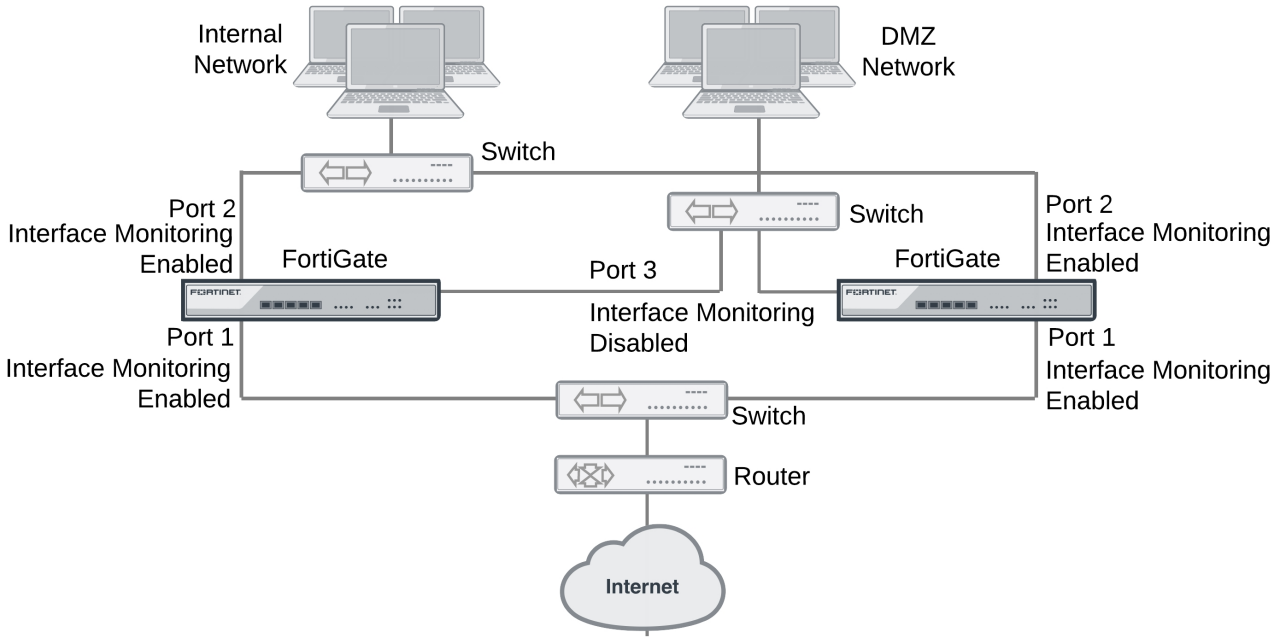
Every time a monitored interface fails, the cluster repeats the processes described above. If multiple monitored interfaces fail on more than one cluster unit, the cluster continues to negotiate to select a primary unit that can provide the most network connections.

Example link failover scenarios

For the following examples, assume a cluster configuration consisting of two FortiGate units (FGT_1 and FGT_2) connected to three networks: internal using port2, external using port1, and DMZ using port3. In the HA configuration, the device priority of FGT_1 is set higher than the unit priority of FGT_2.

The cluster processes traffic flowing between the internal and external networks, between the internal and DMZ networks, and between the external and DMZ networks. If there are no link failures, FGT1 becomes the primary unit because it has the highest device priority.

Sample link failover scenario topology



Example the port1 link on FGT_1 fails

If the port1 link on FGT_1 fails, FGT_2 becomes primary unit because it has fewer interfaces with a link failure. If the cluster is operating in active-active mode, the cluster load balances traffic between the internal network (port2) and the DMZ network (port3). Traffic between the Internet (port1) and the internal network (port2) and between the Internet (port1) and the DMZ network (port3) is processed by the primary unit only.

Example port2 on FGT_1 and port1 on FGT_2 fail

If port2 on FGT_1 and port1 on FGT_2 fail, then FGT_1 becomes the primary unit. After both of these link failures, both cluster units have the same monitor priority. So the cluster unit with the highest device priority (FGT_1) becomes the primary unit.

Only traffic between the Internet (port1) and DMZ (port3) networks can pass through the cluster and the traffic is handled by the primary unit only. No load balancing will occur if the cluster is operating in active-active mode.

Subsecond failover

On FortiGate models 395xB and 3x40B HA link failover supports subsecond failover (that is a failover time of less than one second). Subsecond failover is available for interfaces that can issue a link failure system call when the interface goes down. When an interface experiences a link failure and sends the link failure system call, the FGCP receives the system call and initiates a link failover.

For interfaces that do not support subsecond failover, port monitoring regularly polls the connection status of monitored interfaces. When a check finds that an interface has gone down, port monitoring causes a link failover. Subsecond failover results in a link failure being detected sooner because the system doesn't have to wait for the next poll to find out about the failure.

Subsecond failover can accelerate HA failover to reduce the link failover time to less than one second under ideal conditions. Actual failover performance may be vary depending on traffic patterns and network configuration. For example, some network devices may respond slowly to an HA failover.

No configuration changes are required to support subsecond failover. However, for best subsecond failover results, the recommended heartbeat interval is 100ms and the recommended lost heartbeat threshold is 5 (see Modifying heartbeat timing on page 1462).

```
config system ha
   set hb-lost-threshold 5
   set hb-interval 1
end
```

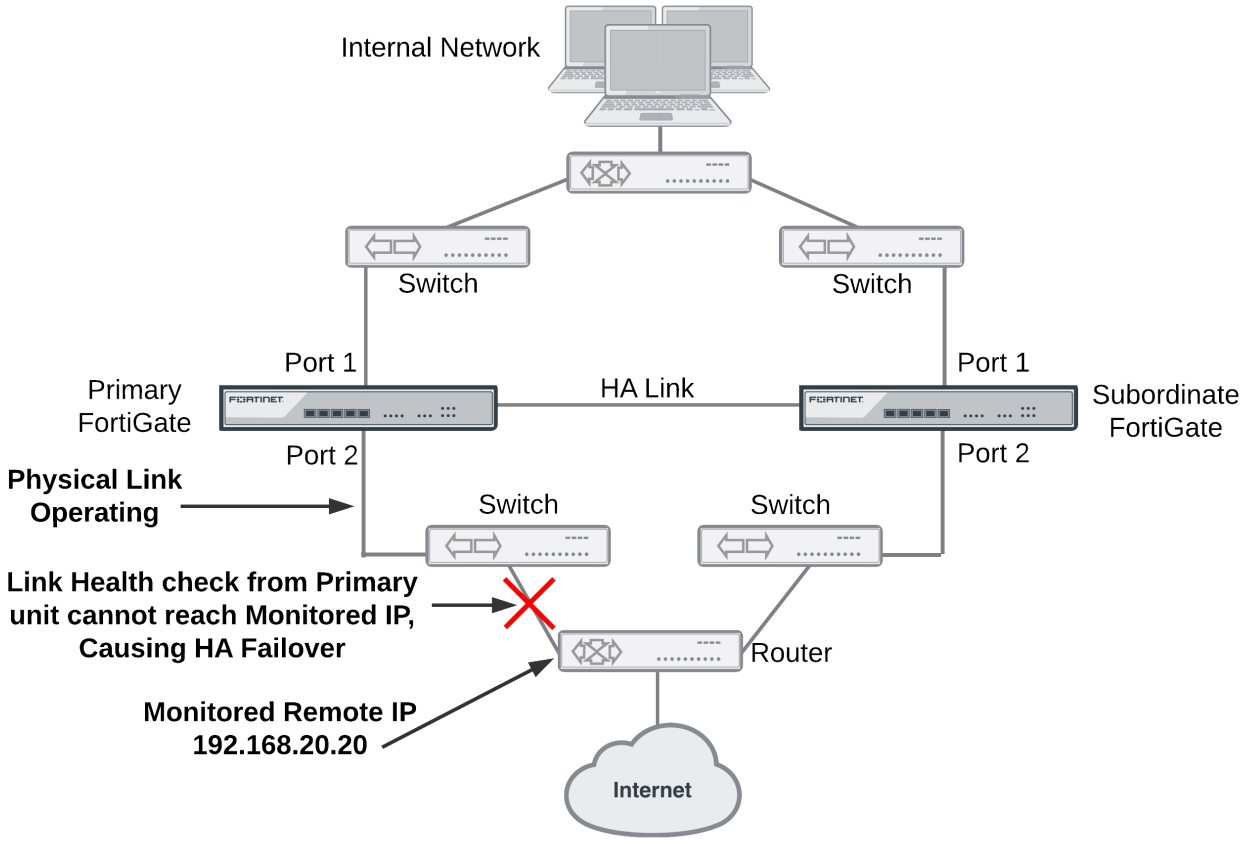
For information about how to reduce failover times, see Failover performance on page 1506.

Remote link failover

Remote link failover (also called remote IP monitoring) is similar to HA port monitoring and link health monitoring (also known as dead gateway detection). Port monitoring causes a cluster to failover if a monitored primary unit interface fails or is disconnected. Remote IP monitoring uses link health monitors configured for FortiGate interfaces on the primary unit to test connectivity with IP addresses of network devices. Usually these would be IP addresses of network devices not directly connected to the cluster. For example, a downstream router. Remote IP monitoring causes a failover if one or more of these remote IP addresses does not respond to link health checking.

By being able to detect failures in network equipment not directly connected to the cluster, remote IP monitoring can be useful in a number of ways depending on your network configuration. For example, in a full mesh HA configuration, with remote IP monitoring, the cluster can detect failures in network equipment that is not directly connected to the cluster but that would interrupt traffic processed by the cluster if the equipment failed.

Example HA remote IP monitoring topology



In the simplified example topology shown above, the switch connected directly to the primary unit is operating normally but the link on the other side of the switches fails. As a result traffic can no longer flow between the primary unit and the Internet.

To detect this failure you can create a link health monitor for port2 that causes the primary unit to test connectivity to 192.168.20.20. If the health monitor cannot connect to 192.268.20.20 the cluster to fails over and the subordinate unit becomes the new primary unit. After the failover, the health check monitor on the new primary unit can connect to 192.168.20.20 so the failover maintains connectivity between the internal network and the Internet through the cluster.

To configure remote IP monitoring

1. Enter the following commands to configure HA remote monitoring for the example topology.
   - Enter the `pingserver-monitor-interface` keyword to enable HA remote IP monitoring on port2.
   - Leave the `pingserver-failover-threshold` set to the default value of 5. This means a failover occurs if the link health monitor doesn't get a response after 5 attempts.

- Enter the `pingserver-flip-timeout` keyword to set the flip timeout to 120 minutes. After a failover, if HA remote IP monitoring on the new primary unit also causes a failover, the flip timeout prevents the failover from occurring until the timer runs out. Setting the `pingserver-flip-timeout` to 120 means that remote IP monitoring can only cause a failover every 120 minutes. This flip timeout is required to prevent repeating failovers if remote IP monitoring causes a failover from all cluster units because none of the cluster units can connect to the monitored IP addresses.

```
config system ha
   set pingserver-monitor-interface port2
   set pingserver-failover-threshold 5
   set pingserver-flip-timeout 120
end
```

2. Enter the following commands to add a link health monitor for the port2 interface and to set HA remote IP monitoring priority for this link health monitor.
   - Enter the `detectserver` keyword to set the health monitor server IP address to 192.168.20.20.
   - Leave the `ha-priority` keyword set to the default value of 1. You only need to change this priority if you change the HA `pingserver-failover-threshold`. The `ha-priority` setting is not synchronized among cluster units.

The `ha-priority` setting is not synchronized among cluster units. So if you want to change the `ha-priority` setting you must change it separately on each cluster unit. Otherwise it will remain set to the default value of 1.

   - Use the `interval` keyword to set the time between link health checks and use the `failtime` keyword to set the number of times that a health check can fail before a failure is detected (the failover threshold). The following example reduces the failover threshold to 2 but keeps the health check interval at the default value of 5.

```
config system link-monitor
   edit ha-link-monitor
      set server 192.168.20.20
      set srcintf port2
      set ha-priority 1
      set interval 5
      set failtime 2
   end
```

You can also do this from the web-based manager by going to **Router > Static > Settings > Link Health Monitor**, selecting **Create New** and set **Interface** to port2, **Probe Type** to Ping, **Server** to 192.168.20.20, **Probe Interval** to 5, **Failure Threshold** to 2 and **HA Priority** to 1.

Adding HA remote IP monitoring to multiple interfaces

You can enable HA remote IP monitoring on multiple interfaces by adding more interface names to the `pingserver-monitor-interface` keyword. If your FortiGate configuration includes VLAN interfaces, aggregate interfaces and other interface types, you can add the names of these interfaces to the `pingserver-monitor-interface` keyword to configure HA remote IP monitoring for these interfaces.

For example, enable remote IP monitoring for interfaces named port2, port20, and vlan_234:

```
config system ha
   set pingserver-monitor-interface port2 port20 vlan_234
```

```
    set pingserver-failover-threshold 10
    set pingserver-flip-timeout 120
end
```

Then configure health monitors for each of these interfaces. In the following example, default values are accepted for all settings other than the server IP address.

```
config system link-monitor
    edit port2
        set srcintf port2
        set server 192.168.20.20
    next
    edit port20
        set srcintf port20
        set server 192.168.20.30
    next
    edit vlan_234
        set srcintf vlan_234
        set server 172.20.12.10
    end
```

Changing the link monitor failover threshold

If you have multiple link monitors you may want a failover to occur only if more than one of them fails.

For example, you may have 3 link monitors configured on three interfaces but only want a failover to occur if two of the link monitors fail. To do this you must set the HA priorities of the link monitors and the HA `pingserver-failover-threshold` so that the priority of one link monitor is less than the failover threshold but the added priorities of two link monitors is equal to or greater than the failover threshold. Failover occurs when the HA priority of all failed link monitors reaches or exceeds the threshold.

For example, set the failover threshold to 10 and monitor three interfaces:

```
config system ha
    set pingserver-monitor-interface port2 port20 vlan_234
    set pingserver-failover-threshold 10
    set pingserver-flip-timeout 120
end
```

Then set the HA priority of link monitor server to 5.

The HA Priority (`ha-priority`) setting is not synchronized among cluster units. In the following example, you must set the HA priority to 5 by logging into each cluster unit.

```
config system link-monitor
    edit port2
        set server 192.168.20.20
        set ha-priority 5
    next
    edit port20
        set server 192.168.20.30
        set ha-priority 5
    next
    edit vlan_234
        set server 172.20.12.10
        set ha-priority 5
    end
```

If only one of the link monitors fails, the total link monitor HA priority will be 5, which is lower than the failover threshold so a failover will not occur. If a second link monitor fails, the total link monitor HA priority of 10 will equal the failover threshold, causing a failover.

By adding multiple link monitors and setting the HA priorities for each, you can fine tune remote IP monitoring. For example, if it is more important to maintain connections to some networks you can set the HA priorities higher for these link monitors. And if it is less important to maintain connections to other networks you can set the HA priorities lower for these link monitors. You can also adjust the failover threshold so that if the cluster cannot connect to one or two high priority IP addresses a failover occurs. But a failover will not occur if the cluster cannot connect to one or two low priority IP addresses.

Monitoring multiple IP addresses from one interface

You can add multiple IP addresses to a single link monitor to use HA remote IP monitoring to monitor more than one IP address from a single interface. If you add multiple IP addresses, the health checking will be with all of the addresses at the same time. The link monitor only fails when no responses are received from all of the addresses.

```
config system link-monitor
   edit port2
      set server 192.168.20.20 192.168.20.30 172.20.12.10
   end
```

Flip timeout

The HA remote IP monitoring configuration also involves setting a flip timeout. The flip timeout is required to reduce the frequency of failovers if, after a failover, HA remote IP monitoring on the new primary unit also causes a failover. This can happen if the new primary unit cannot connect to one or more of the monitored remote IP addresses. The result could be that until you fix the network problem that blocks connections to the remote IP addresses, the cluster will experience repeated failovers. You can control how often the failovers occur by setting the flip timeout. The flip timeout stops HA remote IP monitoring from causing a failover until the primary unit has been operating for the duration of the flip timeout.

If you set the flip timeout to a relatively high number of minutes you can find and repair the network problem that prevented the cluster from connecting to the remote IP address without the cluster experiencing very many failovers. Even if it takes a while to detect the problem, repeated failovers at relatively long time intervals do not usually disrupt network traffic.

Use the following command to set the flip timeout to 3 hours (360 minutes):

```
config system ha
   set pingserver-flip-timeout 360
end
```

Detecting HA remote IP monitoring failovers

Just as with any HA failover, you can detect HA remote IP monitoring failovers by using SNMP to monitor for HA traps. You can also use alert email to receive notifications of HA status changes and monitor log messages for HA failover log messages. In addition, FortiGate units send the critical log message `Ping Server is down` when a ping server fails. The log message includes the name of the interface that the ping server has been added to.

Session failover (session pick-up)

Session failover means that a cluster maintains active network TCP and IPsec VPN sessions (including NAT sessions) after a device or link failover. You can also configure session failover to maintain UDP and ICMP sessions. Session failover does not failover multicast, or SSL VPN sessions.

FortiGate HA does not support session failover by default. To enable session failover go to **System > Config > HA** and select **Enable Session Pick-up**.

From the CLI enter:

```
config system ha
   set session-pickup enable
end
```

To support session failover, when **Enable Session Pick-up** is selected, the FGCP maintains an HA session table for most TCP communication sessions being processed by the cluster and synchronizes this session table with all cluster units. If a cluster unit fails, the HA session table information is available to the remaining cluster units and these cluster units use this session table to resume most of the TCP sessions that were being processed by the failed cluster unit without interruption.

If session pickup is enabled, you can use the following command to also enable UDP and ICMP session failover:

```
config system ha
   set session-pickup-connectionless enable
end
```

You must enable session pickup for session failover protection. If you do not require session failover protection, leaving session pickup disabled may reduce CPU usage and reduce HA heartbeat network bandwidth usage.

If session pickup is not selected

If **Enable Session Pick-up** is not selected, the FGCP does not maintain an HA session table and most TCP sessions do not resume after a failover. After a device or link failover all sessions are briefly interrupted and must be re-established at the application level after the cluster renegotiates.

Many protocols can successfully restart sessions with little, if any, loss of data. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Since most HTTP sessions are very short, in most cases they will not even notice an interruption unless they are downloading large files. Users downloading a large file may have to restart their download after a failover.

Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.

Some sessions may resume after a failover whether or not enable session pick-up is selected:

- UDP, ICMP, multicast and broadcast packet session failover on page 1500
- FortiOS Carrier GTP session failover on page 1500
- Active-active HA subordinate units sessions can resume after a failover on page 1501

Improving session synchronization performance

Two HA configuration options are available to reduce the performance impact of enabling session pickup. They include reducing the number of sessions that are synchronized by adding a session pickup delay and using more FortiGate interfaces for session synchronization.

Reducing the number of sessions that are synchronized

Enable the `session-pickup-delay` CLI option to reduce the number of sessions that are synchronized by synchronizing sessions only if they remain active for more than 30 seconds. Enabling this option could greatly reduce the number of sessions that are synchronized if a cluster typically processes very many short duration sessions, which is typical of most HTTP traffic for example.

Use the following command to enable a 30 second session pickup delay:

```
config system ha
   set session-pickup-delay enable
end
```

Enabling session pickup delay means that if a failover occurs more sessions may not be resumed after a failover. In most cases short duration sessions can be restarted with only a minor traffic interruption. However, if you notice too many sessions not resuming after a failover you might want to disable this setting.

Using multiple FortiGate interfaces for session synchronization

Using the `session-sync-dev` option you can select one or more FortiGate interfaces to use for synchronizing sessions as required for session pickup. Normally session synchronization occurs over the HA heartbeat link. Using this HA option means only the selected interfaces are used for session synchronization and not the HA heartbeat link. If you select more than one interface, session synchronization traffic is load balanced among the selected interfaces.

Moving session synchronization from the HA heartbeat interface reduces the bandwidth required for HA heartbeat traffic and may improve the efficiency and performance of the cluster, especially if the cluster is synchronizing a large number of sessions. Load balancing session synchronization among multiple interfaces can further improve performance and efficiency if the cluster is synchronizing a large number of sessions.

Use the following command to perform cluster session synchronization using the port10 and port12 interfaces.

```
config system ha
   set session-sync-dev port10 port12
end
```

Session synchronization packets use Ethertype 0x8892. The interfaces to use for session synchronization must be connected together either directly using the appropriate cable (possible if there are only two units in the cluster) or using switches. If one of the interfaces becomes disconnected the cluster uses the remaining interfaces for session synchronization. If all of the session synchronization interfaces become disconnected, session synchronization reverts back to using the HA heartbeat link. All session synchronization traffic is between the primary unit and each subordinate unit.

Since large amounts of session synchronization traffic can increase network congestion, it is recommended that you keep this traffic off of your network by using dedicated connections for it.

Synchronizing GTP sessions to support GTP tunnel failover

FortiOS Carrier GPRS Tunneling Protocol (GTP) sessions are not normally synchronized by the FGCP, even if you enable session pickup. You can provide GTP session synchronization by using the `session-sync-dev` command to select one or two session sync interfaces. You must also connect these interfaces together either with direct connections or using switches.

You can also use the command, `diagnose firewall gtp hash-stat` to display GTP hash stat separately.

Session failover not supported for all sessions

Most of the features applied to sessions by FortiGate security profile functionality require the FortiGate unit to maintain very large amounts of internal state information for each session. The FGCP does not synchronize internal state information for the following security profile features, so the following types of sessions will not resume after a failover:

- Virus scanning of HTTP, HTTPS, FTP, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, IM, CIFS, and NNTP sessions,
- Web filtering and FortiGuard Web Filtering of HTTP and HTTPS sessions,
- Spam filtering of IMAP, IMAPS, POP3, POP3S, SMTP, and SMTPS sessions,
- DLP scanning of IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, SIP, SIMPLE, and SCCP sessions,
- DLP archiving of HTTP, HTTPS, FTP, IMAP, IMAPS, POP3, SMTP, SMTPS, IM, NNTP, AIM, ICQ, MSN, Yahoo! IM, SIP, SIMPLE, and SCCP signal control sessions,

Active-active clusters can resume some of these sessions after a failover. See Active-active HA subordinate units sessions can resume after a failover on page 1501 for details.

If you use these features to protect most of the sessions that your cluster processes, enabling session failover may not actually provide significant session failover protection.

TCP sessions that are not being processed by these security profile features resume after a failover even if these sessions are accepted by security policies with security profile options configured. Only TCP sessions that are actually being processed by these security profile features do not resume after a failover. For example:

- TCP sessions that are not virus scanned, web filtered, spam filtered, content archived, or are not SIP, SIMPLE, or SCCP signal traffic resume after a failover, even if they are accepted by a security policy with security profile options enabled. For example, SNMP TCP sessions resume after a failover because FortiOS does not apply any security profile options to SNMP sessions.
- TCP sessions for a protocol for which security profile features have not been enabled resume after a failover even if they are accepted by a security policy with security profile features enabled. For example, if you have not enabled any antivirus or content archiving settings for FTP, FTP sessions resume after a failover.

The following security profile features do not affect TCP session failover:

- IPS does not affect session failover. Sessions being scanned by IPS resume after a failover. After a failover; however, IPS can only perform packet-based inspection of resumed sessions; reducing the number of vulnerabilities that IPS can detect. This limitation only applies to in-progress resumed sessions.
- Application control does not affect session failover. Sessions that are being monitored by application control resume after a failover.
- Logging enabled form security profile features does not affect session failover. security profile logging writes log messages for security profile events; such as when a virus is found by antivirus scanning, when Web Filtering blocks a URL, and so on. Logging does not enable features that would prevent sessions from being failed over, logging just reports on the activities of enabled features.

If more than one security profile feature is applied to a TCP session, that session will not resume after a failover as long as one of the security profile features prevents session failover. For example:

- Sessions being scanned by IPS and also being virus scanned do not resume after a failover.
- Sessions that are being monitored by application control and that are being DLP archived or virus scanned will not resume after a failover.

IPv6, NAT64, and NAT66 session failover

The FGCP supports IPv6, NAT64, and NAT66 session failover, if session pickup is enabled, these sessions are synchronized between cluster members and after an HA failover the sessions will resume with only minimal interruption.

SIP session failover

The FGCP supports SIP session failover (also called stateful failover) for active-passive HA. To support SIP session failover, create a standard HA configuration and select **Enable Session Pick-up** option.

SIP session failover replicates SIP states to all cluster units. If an HA failover occurs, all in-progress SIP calls (setup complete) and their RTP flows are maintained and the calls will continue after the failover with minimal or no interruption.

SIP calls being set up at the time of a failover may lose signaling messages. In most cases the SIP clients and servers should use message retransmission to complete the call setup after the failover has completed. As a result, SIP users may experience a delay if their calls are being set up when an HA a failover occurs. But in most cases the call setup should be able to continue after the failover.

Explicit web proxy, WCCP, and WAN optimization session failover

Similar to security profile sessions, the explicit web proxy, WCCP and WAN optimization features all require the FortiGate unit to maintain very large amounts of internal state information for each session. This information is not maintained and these sessions do not resume after a failover.

SSL offloading and HTTP multiplexing session failover

SSL offloading and HTTP multiplexing are both enabled from firewall virtual IPs and firewall load balancing. Similar to the features applied by security profile, SSL offloading and HTTP multiplexing requires the FortiGate unit to maintain very large amounts of internal state information for each session. Sessions accepted by security policies containing virtual IPs or virtual servers with SSL offloading or HTTP multiplexing enabled do not resume after a failover.

IPsec VPN session failover

Session failover is supported for all IPsec VPN tunnels. To support IPsec VPN tunnel failover, when an IPsec VPN tunnel starts, the FGCP distributes the SA and related IPsec VPN tunnel data to all cluster units.

SSL VPN session failover and SSL VPN authentication failover

Session failover is not supported for SSL VPN tunnels. However, authentication failover is supported for the communication between the SSL VPN client and the FortiGate unit. This means that after a failover, SSL VPN clients can re-establish the SSL VPN session between the SSL VPN client and the FortiGate unit without having to authenticate again.

However, all sessions inside the SSL VPN tunnel that were running before the failover are stopped and have to be restarted. For example, file transfers that were in progress would have to be restarted. As well, any communication sessions with resources behind the FortiGate unit that are started by an SSL VPN session have to be restarted.

To support SSL VPN cookie failover, when an SSL VPN session starts, the FGCP distributes the cookie created to identify the SSL VPN session to all cluster units.

PPTP and L2TP VPN sessions

PPTP and L2TP VPNs are supported in HA mode. For a cluster you can configure PPTP and L2TP settings and you can also add security policies to allow PPTP and L2TP pass through. However, the FGCP does not provide session failover for PPTP or L2TP. After a failover, all active PPTP and L2TP sessions are lost and must be restarted.

UDP, ICMP, multicast and broadcast packet session failover

By default, even with session pickup enabled, the FGCP does not maintain a session table for UDP, ICMP, multicast, or broadcast packets. So the cluster does not specifically support failover of these packets.

Some UDP traffic can continue to flow through the cluster after a failover. This can happen if, after the failover, a UDP packet that is part of an already established communication stream matches a security policy. Then a new session will be created and traffic will flow. So after a short interruption, UDP sessions can appear to have failed over. However, this may not be reliable for the following reasons:

- UDP packets in the direction of the security policy must be received before reply packets can be accepted. For example, if a port1 -> port2 policy accepts UDP packets, UDP packets received at port2 destined for the network connected to port1 will not be accepted until the policy accepts UDP packets at port1 that are destined for the network connected to port2. So, if a user connects from an internal network to the Internet and starts receiving UDP packets from the Internet (for example streaming media), after a failover the user will not receive any more UDP packets until the user re-connects to the Internet site.
- UDP sessions accepted by NAT policies will not resume after a failover because NAT will usually give the new session a different source port. So only traffic for UDP protocols that can handle the source port changing during a session will continue to flow.

You can however, enable session pickup for UDP and ICMP packets by enabling session pickup for TCP sessions and then enabling session pickup for connectionless sessions:

```
config system ha
   set session-pickup enable
   set session-pickup-connectionless enable
end
```

This configuration causes the cluster units to synchronize UDP and ICMP session tables and if a failover occurs UDP and ICMP sessions are maintained.

FortiOS Carrier GTP session failover

FortiOS Carrier HA supports GTP session failover. The primary unit synchronizes the GTP tunnel state to all cluster units after the GTP tunnel setup is completed. After the tunnel setup is completed, GTP sessions use UDP and HA does not synchronize UDP sessions to all cluster units. However, similar to other UDP sessions, after a failover, since the new primary unit will have the GTP tunnel state information, GTP UDP sessions using the same tunnel can continue to flow with some limitations.

The limitation on packets continuing to flow is that there has to be a security policy to accept the packets. For example, if the FortiOS Carrier unit has an internal to external security policy, GTP UDP sessions using an established tunnel that are received by the internal interface are accepted by the security policy and can continue to flow. However, GTP UDP packets for an established tunnel that are received at the external interface cannot flow until packets from the same tunnel are received at the internal interface.

If you have bi-directional policies that accept GTP UDP sessions then traffic in either direction that uses an established tunnel can continue to flow after a failover without interruption.

Active-active HA subordinate units sessions can resume after a failover

In an active-active cluster, subordinate units process sessions. After a failover, all cluster units that are still operating may be able to continue processing the sessions that they were processing before the failover. These sessions are maintained because after the failover the new primary unit uses the HA session table to continue to send session packets to the cluster units that were processing the sessions before the failover. Cluster units maintain their own information about the sessions that they are processing and this information is not affected by the failover. In this way, the cluster units that are still operating can continue processing their own sessions without loss of data.

The cluster keeps processing as many sessions as it can. But some sessions can be lost. Depending on what caused the failover, sessions can be lost in the following ways:

- A cluster unit fails (the primary unit or a subordinate unit). All sessions that were being processed by that cluster unit are lost.
- A link failure occurs. All sessions that were being processed through the network interface that failed are lost.

This mechanism for continuing sessions is not the same as session failover because:

- Only the sessions that can be maintained are maintained.
- The sessions are maintained on the same cluster units and not re-distributed.
- Sessions that cannot be maintained are lost.

WAN optimization and HA

You can configure WAN optimization on a FortiGate HA cluster. The recommended HA configuration for WAN optimization is active-passive mode. Also, when the cluster is operating, all WAN optimization sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance WAN optimization sessions. HA also does not support WAN optimization session failover.

In a cluster, the primary unit only stores web cache and byte cache databases. These databases are not synchronized to the subordinate units. So, after a failover, the new primary unit must rebuild its web and byte caches. As well, the new primary unit cannot connect to a SAS partition that the failed primary unit used.

Rebuilding the byte caches can happen relatively quickly because the new primary unit gets byte cache data from the other FortiGate units that it is participating with in WAN optimization tunnels.

Failover and attached network equipment

It normally takes a cluster approximately 6 seconds to complete a failover. However, the actual failover time experienced by your network users may depend on how quickly the switches connected to the cluster interfaces accept the cluster MAC address update from the primary unit. If the switches do not recognize and accept the gratuitous ARP packets and update their MAC forwarding table, the failover time will increase.

Also, individual session failover depends on whether the cluster is operating in active-active or active-passive mode, and whether the content of the traffic is to be virus scanned. Depending on application behavior, it may take a TCP session a longer period of time (up to 30 seconds) to recover completely.

Monitoring cluster units for failover

You can use logging and SNMP to monitor cluster units for failover. Both the primary and subordinate units can be configured to write log messages and send SNMP traps if a failover occurs. You can also log into the cluster web-based manager and CLI to determine if a failover has occurred.

NAT/Route mode active-passive cluster packet flow

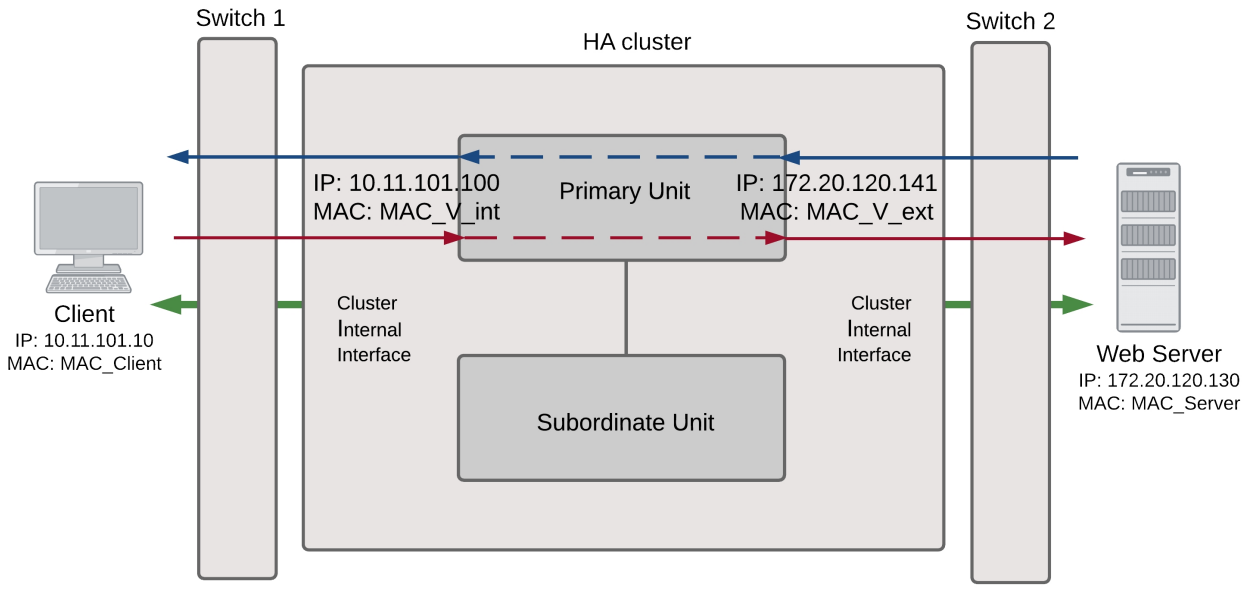
This section describes how packets are processed and how failover occurs in an active-passive HA cluster running in NAT/Route mode. In the example, the NAT/Route mode cluster acts as the internet firewall for a client computer's internal network. The client computer's default route points at the IP address of the cluster internal interface. The client connects to a web server on the Internet. Internet routing routes packets from the cluster external interface to the web server, and from the web server to the cluster external interface.

In an active-passive cluster operating in NAT/Route mode, four MAC addresses are involved in communication between the client and the web server when the primary unit processes the connection:

- Internal virtual MAC address (MAC_V_int) assigned to the primary unit internal interface,
- External virtual MAC address (MAC_V_ext) assigned to the primary unit external interface,
- Client MAC address (MAC_Client),
- Server MAC address (MAC_Server),

In NAT/Route mode, the HA cluster works as a gateway when it responds to ARP requests. Therefore, the client and server only know the gateway MAC addresses. The client only knows the cluster internal virtual MAC address (MAC_V_int) and the server only know the cluster external virtual MAC address (MAC_V_int).

NAT/Route mode active-passive packet flow



Packet flow from client to web server

1. The client computer requests a connection from 10.11.101.10 to 172.20.120.130.
2. The default route on the client computer recognizes 10.11.101.100 (the cluster IP address) as the gateway to the external network where the web server is located.
3. The client computer issues an ARP request to 10.11.101.100.
4. The primary unit intercepts the ARP request, and responds with the internal virtual MAC address (MAC_V_int) which corresponds to its IP address of 10.11.101.100.
5. The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
Source	10.11.101.10	MAC_Client
Destination	172.20.120.130	MAC_V_int

6. The primary unit processes the packet.
7. The primary unit forwards the packet from its external interface to the web server.

	IP address	MAC address
Source	172.20.120.141	MAC_V_ext
Destination	172.20.120.130	MAC_Server

8. The primary unit continues to process packets in this way unless a failover occurs.

Packet flow from web server to client

1. When the web server responds to the client's packet, the cluster external interface IP address (172.20.120.141) is recognized as the gateway to the internal network.
2. The web server issues an ARP request to 172.20.120.141.
3. The primary unit intercepts the ARP request, and responds with the external virtual MAC address (MAC_V_ext) which corresponds its IP address of 172.20.120.141.
4. The web server then sends response packets to the primary unit external interface.

	IP address	MAC address
Source	172.20.120.130	MAC_Server
Destination	172.20.120.141	MAC_V_ext

5. The primary unit processes the packet.
6. The primary unit forwards the packet from its internal interface to the client.

	IP address	MAC address
Source	172.20.120.130	MAC_V_int
Destination	10.11.101.10	MAC_Client

7. The primary unit continues to process packets in this way unless a failover occurs.

When a failover occurs

The following steps are followed after a device or link failure of the primary unit causes a failover.

1. If the primary unit fails the subordinate unit becomes the primary unit.
2. The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC addresses.
   The new primary unit has the same IP addresses and MAC addresses as the failed primary unit.
3. The new primary units sends gratuitous ARP packets from the internal interface to the 10.11.101.0 network to associate its internal IP address with the internal virtual MAC address.
4. The new primary units sends gratuitous ARP packets to the 172.20.120.0 to associate its external IP address with the external virtual MAC address.
5. Traffic sent to the cluster is now received and processed by the new primary unit.
   If there were more than two cluster units in the original cluster, these remaining units would become subordinate units.

Transparent mode active-passive cluster packet flow

This section describes how packets are processed and how failover occurs in an active-passive HA cluster running in Transparent mode. The cluster is installed on an internal network in front of a mail server and the client connects to the mail server through the Transparent mode cluster.

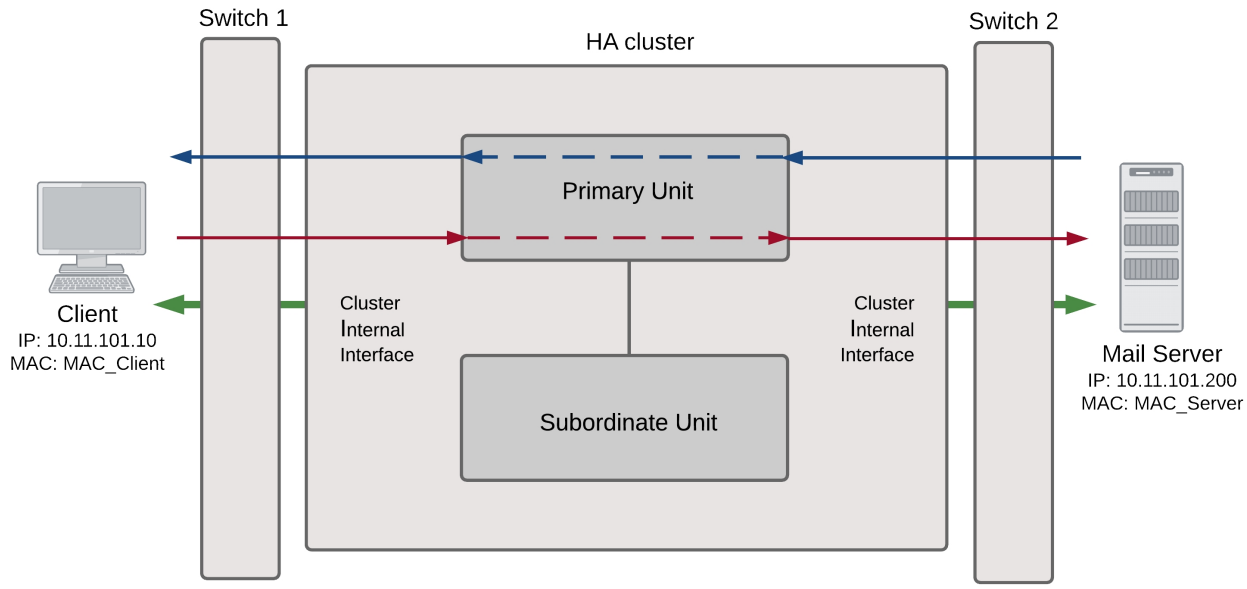
In an active-passive cluster operating in Transparent mode, two MAC addresses are involved in the communication between a client and a server when the primary unit processes a connection:

- Client MAC address (MAC_Client)
- Server MAC address (MAC_Server)

The HA virtual MAC addresses are not directly involved in communication between the client and the server. The client computer sends packets to the mail server and the mail server sends responses. In both cases the packets are intercepted and processed by the cluster.

The cluster's presence on the network is transparent to the client and server computers. The primary unit sends gratuitous ARP packets to Switch 1 that associate all MAC addresses on the network segment connected to the cluster external interface with the HA virtual MAC address. The primary unit also sends gratuitous ARP packets to Switch 2 that associate all MAC addresses on the network segment connected to the cluster internal interface with the HA virtual MAC address. In both cases, this results in the switches sending packets to the primary unit interfaces.

Transparent mode active-passive packet flow



Packet flow from client to mail server

1. The client computer requests a connection from 10.11.101.10 to 110.11.101.200.
2. The client computer issues an ARP request to 10.11.101.200.
3. The primary unit forwards the ARP request to the mail server.
4. The mail server responds with its MAC address (MAC_Server) which corresponds to its IP address of 10.11.101.200. The primary unit returns the ARP response to the client computer.
5. The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
Source	10.11.101.10	MAC_Client
Destination	10.11.101.200	MAC_Server

6. The primary unit processes the packet.
7. The primary unit forwards the packet from its external interface to the mail server.

	IP address	MAC address
Source	10.11.101.10	MAC_Client
Destination	10.11.101.200	MAC_Server

8. The primary unit continues to process packets in this way unless a failover occurs.

Packet flow from mail server to client

1. To respond to the client computer, the mail server issues an ARP request to 10.11.101.10.
2. The primary unit forwards the ARP request to the client computer.
3. The client computer responds with its MAC address (MAC_Client) which corresponds to its IP address of 10.11.101.10. The primary unit returns the ARP response to the mail server.
4. The mail server's response packet reaches the primary unit external interface.

	IP address	MAC address
Source	10.11.101.200	MAC_Server
Destination	10.11.101.10	MAC_Client

5. The primary unit processes the packet.
6. The primary unit forwards the packet from its internal interface to the client.

	IP address	MAC address
Source	10.11.101.200	MAC_Server
Destination	10.11.101.10	MAC_Client

7. The primary unit continues to process packets in this way unless a failover occurs.

When a failover occurs

The following steps are followed after a device or link failure of the primary unit causes a failover.

1. If the primary unit fails, the subordinate unit negotiates to become the primary unit.
2. The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.
3. The new primary units sends gratuitous ARP packets to switch 1 to associate its MAC address with the MAC addresses on the network segment connected to the external interface.
4. The new primary units sends gratuitous ARP packets to switch 2 to associate its MAC address with the MAC addresses on the network segment connected to the internal interface.
5. Traffic sent to the cluster is now received and processed by the new primary unit.

   If there were more than two cluster units in the original cluster, these remaining units would become subordinate units.

Failover performance

This section describes the designed device and link failover times for a FortiGate cluster and also shows results of a failover performance test.

Device failover performance

By design FGCP device failover time is 2 seconds for a two-member cluster with ideal network and traffic conditions. If subsecond failover is enabled the failover time can drop below 1 second.

All cluster units regularly receive HA heartbeat packets from all other cluster units over the HA heartbeat link. If any cluster unit does not receive a heartbeat packet from any other cluster unit for 2 seconds, the cluster unit that has not sent heartbeat packets is considered to have failed.

It may take another few seconds for the cluster to negotiate and re-distribute communication sessions. Typically if subsecond failover is not enabled you can expect a failover time of 9 to 15 seconds depending on the cluster and network configuration. The failover time can also be increased by more complex configurations and or configurations with network equipment that is slow to respond.

You can change the `hb-lost-threshold` to increase or decrease the device failover time. See Modifying heartbeat timing on page 1462 for information about using `hb-lost-threshold`, and other heartbeat timing settings.

Link failover performance

Link failover time is controlled by how long it takes for a cluster to synchronize the cluster link database. When a link failure occurs, the cluster unit that experienced the link failure uses HA heartbeat packets to broadcast the updated link database to all cluster units. When all cluster units have received the updated database the failover is complete.

It may take another few seconds for the cluster to negotiate and re-distribute communication sessions.

Reducing failover times

- Keep the network configuration as simple as possible with as few as possible network connections to the cluster.
- If possible operate the cluster in Transparent mode.
- Use high-performance switches to that the switches failover to interfaces connected to the new primary unit as quickly as possible.
- Use accelerated FortiGate interfaces. In some cases accelerated interfaces will reduce failover times.
- Make sure the FortiGate unit sends multiple gratuitous arp packets after a failover. In some cases, sending more gratuitous arp packets will cause connected network equipment to recognize the failover sooner. To send 10 gratuitous arp packets:

```
config system ha
   set arps 10
end
```

- Reduce the time between gratuitous arp packets. This may also caused connected network equipment to recognize the failover sooner. To send 50 gratuitous arp packets with 1 second between each packet:

```
config system ha
   set arps 50
   set arps-interval 1
end
```

- Reduce the number of lost heartbeat packets and reduce the heartbeat interval timers to be able to more quickly detect a device failure. To set the lost heartbeat threshold to 3 packets and the heartbeat interval to 100 milliseconds:

```
config system ha
   set hb-interval 1
   set hb-lost-threshold 3
end
```

- Reduce the hello state hold down time to reduce the amount of the time the cluster waits before transitioning from the hello to the work state. To set the hello state hold down time to 5 seconds:

```
config system ha
   set helo-holddown 5
end
```

- Enable sending a link failed signal after a link failover to make sure that attached network equipment responds a quickly as possible to a link failure. To enable the link failed signal:

```
config system ha
   set link-failed-signal enable
end
```

HA and load balancing

FGCP active-active (a-a) load balancing distributes network traffic among all of the units in a cluster. Load balancing can improve cluster performance because the processing load is shared among multiple cluster units.

This chapter describes how active-active load balancing works and provides detailed active-active HA NAT/Route and Transparent mode packet flow descriptions.

Load balancing overview

FGCP active-active HA uses a technique similar to unicast load balancing in which the primary unit is associated with the cluster HA virtual MAC addresses and cluster IP addresses. The primary unit is the only cluster unit to receive packets sent to the cluster. The primary unit then uses a load balancing schedule to distribute sessions to all of the units in the cluster (including the primary unit). Subordinate unit interfaces retain their actual MAC addresses and the primary unit communicates with the subordinate units using these MAC addresses. Packets exiting the subordinate units proceed directly to their destination and do not pass through the primary unit first.

By default, active-active HA load balancing distributes proxy-based security profile processing to all cluster units. Proxy-based security profile processing is CPU and memory-intensive, so FGCP load balancing may result in higher throughput because resource-intensive processing is distributed among all cluster units.

Proxy-based security profile processing that is load balanced includes proxy-based virus scanning, proxy-based web filtering, proxy-based email filtering, and proxy-based data leak prevention (DLP) of HTTP, FTP, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, IM, and NNTP, sessions accepted by security policies.

Other features enabled in security policies such as Endpoint security, traffic shaping and authentication have no effect on active-active load balancing.

You can also enable `load-balance-all` to have the primary unit load balance all TCP sessions. Load balancing TCP sessions increases overhead and may actually reduce performance so it is disabled by default. You can also enable `load-balance-udp` to have the primary unit load balance all UDP sessions. Load balancing UDP sessions also increases overhead so it is also disabled by default.

NP4 and NP6 processors can also offload and accelerate load balancing.

During active-active HA load balancing the primary unit uses the configured load balancing schedule to determine the cluster unit that will process a session. The primary unit stores the load balancing information for each load balanced session in the cluster load balancing session table. Using the information in this table, the primary unit can then forward all of the remaining packets in each session to the appropriate cluster unit. The load balancing session table is synchronized among all cluster units.

HTTPS, ICMP, multicast, and broadcast sessions are never load balanced and are always processed by the primary unit. IPS,Application Control, flow-based virus scanning, flow-based web filtering, flow-based DLP, flow-based email filtering, VoIP, IM, P2P, IPsec VPN, HTTPS, SSL VPN, HTTP multiplexing, SSL offloading, WAN optimization, explicit web proxy, and WCCP sessions are also always processed only by the primary unit.

In addition to load balancing, active-active HA also provides the same session, device and link failover protection as active-passive HA. If the primary unit fails, a subordinate unit becomes the primary unit and resumes operating the cluster.

Active-active HA also maintains as many load balanced sessions as possible after a failover by continuing to process the load balanced sessions that were being processed by the cluster units that are still operating. See Active-active HA subordinate units sessions can resume after a failover on page 1501 for more information.

Load balancing schedules

The load balancing schedule controls how the primary unit distributes packets to all cluster units. You can select from the following load balancing schedules.

Schedule	Description
None	No load balancing. Select None when the cluster interfaces are connected to load balancing switches. If you select None, the Primary unit does not load balance traffic and the subordinate units process incoming traffic that does not come from the Primary unit. For all other load balancing schedules, all traffic is received first by the Primary unit, and then forwarded to the subordinate units. The subordinate units only receive and process packets sent from the primary unit.
Hub	Load balancing if the cluster interfaces are connected to a hub. Traffic is distributed to cluster units based on the source IP and destination IP of the packet.
Least-Connection	If the cluster units are connected using switches, select **Least Connection** to distribute network traffic to the cluster unit currently processing the fewest connections.
Round-Robin	If the cluster units are connected using switches, select Round-Robin to distribute network traffic to the next available cluster unit.
Weighted Round-Robin	Similar to round robin, but weighted values are assigned to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic will be more likely to receive new connections than units that are very busy.
Random	If the cluster units are connected using switches, select Random to randomly distribute traffic to cluster units.
IP	Load balancing according to IP address. If the cluster units are connected using switches, select **IP** to distribute traffic to units in a cluster based on the source IP and destination IP of the packet.
IP Port	Load balancing according to IP address and port. If the cluster units are connected using switches, select IP Port to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet.

Once a packet has been propagated to a subordinate unit, all packets are part of that same communication session are also propagated to that same subordinate unit. Traffic is distributed according to communication session, not just according to individual packet.

Any subordinate unit that receives a forwarded packet processes it, without applying load balancing. Note that subordinate units are still considered to be active, because they perform routing, virus scanning, and other FortiGate unit tasks on their share of the traffic. Active subordinate units also share their session and link status

information with all cluster units. The only things that active members do not do is make load balancing decisions.

Even though the primary unit is responsible for the load balancing process, the primary unit still acts like a FortiGate unit in that it processes packets, performing, routing, firewall, virus scanning, and other FortiGate unit tasks on its share of the traffic. Depending on the load balancing schedule used, the primary unit may assign itself a smaller share of the total load.

More about active-active failover

If a subordinate unit fails, the primary unit re-distributes the sessions that the subordinate was processing among the remaining active cluster members. If the primary unit fails, the subordinate units negotiate to select a new primary unit. The new primary unit continues to distribute packets among the remaining active cluster units.

Failover works in a similar way if the cluster consists of only two units. If the primary unit fails the subordinate unit negotiates and becomes the new primary unit. If the subordinate unit fails, the primary unit processes all traffic. In both cases, the single remaining unit continues to function as a primary unit, maintaining the HA virtual MAC address for all of its interfaces.

HTTPS sessions, active-active load balancing, and proxy servers

To prevent HTTPS web filtering problems active-active HA does not load balance HTTPS sessions. The FortiGate unit identifies HTTPS sessions as all sessions received on the HTTPS TCP port. The default HTTPS port is 443. You can go to **Policy & Objects > Policy > SSL/SSH Inspection** to use a custom port for HTTPS sessions. If you change the HTTPS port, the FGCP stops load balancing all sessions that use the custom HTTPS port.

Normally you would not change the HTTPS port. However, if your network uses a proxy server for HTTPS traffic you may have to change to the custom HTTPS port used by your proxy server. If your network uses a proxy server you might also use the same port for both HTTP and HTTPS traffic. In this case you would configure the FortiGate unit to use custom ports for both HTTP and HTTPS traffic. Go to **Policy & Objects > Policy > Proxy Options** to use a custom port for HTTP.

Using the same port for HTTP and HTTPS traffic can cause problems with active-active clusters because active-active clusters always load balance HTTP traffic. If both HTTP and HTTPS use the same port, the active-active cluster cannot differentiate between HTTP and HTTPS traffic and will load balance both.

As mentioned above, load balancing HTTPS traffic may cause problems with HTTPS web filtering. To avoid this problem, you should configure your proxy server to use different ports for HTTP and HTTPS traffic. Then configure your cluster to also use different ports for HTTP and HTTPS.

Selecting a load balancing schedule

You can select the load balancing schedule when initially configuring the cluster and you can change the load balancing schedule at any time while the cluster is operating without affecting cluster operation.

You can select a load balancing schedule from the CLI. Use the following command to select a load balancing schedule:

```
config system ha
   set schedule {hub | ip | ipport | leastconnection | none | random | round-robin
       | weight-round-robin}
end
```

Load balancing TCP and UDP sessions

You can use the following command to configure the cluster to load balance TCP sessions in addition to security profile sessions.

```
config system ha
   set load-balance-all enable
end
```

Enabling `load-balance-all` to add load balancing of TCP sessions may not improve performance because the cluster requires additional overhead to load balance sessions. Load balancing aTCP session usually requires about as much overhead as just processing it. On the other hand, TCP load balancing performance may be improved if your FortiGate unit includes NP4 or NP6 processors.

You can enable `load-balance-all` and monitor network performance to see if it improves. If performance is not improved, you might want to change the HA mode to active-passive since active-active HA is not providing any benefit.

On some FortiGate models you can use the following command to also load balance UDP sessions:

```
config system ha
   set load-balance-udp enable
end
```

Similar to load balancing TCP sessions, load balancing UDP sessions may also not improve performance. Also UDP load balancing performance may ber improved with NP4 and NP6 processors.

Using NP4 or NP6 processors to offload load balancing

FortiGates that include NP4 and NP6 network processors can provide hardware acceleration for active-active HA cluster by offloading load balancing from the primary unit CPU. Network processors are especially useful when load balancing TCP and UDP sessions.

The first packet of every new session is received by the primary unit and the primary unit uses its load balancing schedule to select the cluster unit that will process the new session. This information is passed back to the network processor and all subsequent packets of the same sessions are offloaded to the network processor which sends the packet directly to a subordinate unit. Load balancing is effectively offloaded from the primary unit to the network processor resulting in a faster and more stable active-active cluster.

To take advantage of network processor load balancing acceleration, connect the cluster unit interfaces with network processors to the busiest networks. Connect non-accelerated interfaces to less busy networks. No special FortiOS or HA configuration is required. Network processor acceleration of active-active HA load balancing is supported for any active-active HA configuration or active-active HA load balancing schedule.

Configuring weighted-round-robin weights

You can configure weighted round-robin load balancing for a cluster and configure the static weights for each of the cluster units according to their priority in the cluster. When you set `schedule` to `weight-round-robin` you can use the `weight` option to set the static weight of each cluster unit. The static weight is set according to the priority of each unit in the cluster. A FortiGate HA cluster can contain up to four FortiGate units so you can set up to 4 static weights.

The priority of a cluster unit is determined by its device priority, the number of monitored interfaces that are functioning, its age in the cluster and its serial number. Priorities are used to select a primary unit and to set an

order of all of the subordinate units. Thus the priority order of a cluster unit can change depending on configuration settings, link failures and so on. Since weights are also set using this priority order the weights are independent of specific cluster units but do depend on the role of the each unit in the cluster.

You can use the following command to display the priority order of units in a cluster. The following example displays the priority order for a cluster of 5 FortiGate units:

```
get system ha status
   Model: 620
   Mode: a-p
   Group: 0
   Debug: 0
   ses_pickup: disable
   Master:150 head_office_cla FG600B3908600825 0
   Slave :150 head_office_clb FG600B3908600705 1
   Slave :150 head_office_clc FG600B3908600702 2
   Slave :150 head_office_cld FG600B3908600605 3
   Slave :150 head_office_cle FG600B3908600309 4
   number of vcluster: 1
   vcluster 1: work 169.254.0.1
   Master:0 FG600B3908600825
   Slave :1 FG600B3908600705
   Slave :2 FG600B3908600702
   Slave :3 FG600B3908600605
   Slave :4 FG600B3908600309
```

The cluster units are listed in priority order starting at the 6th output line. The primary unit always has the highest priority and is listed first followed by the subordinate units in priority order. The last 5 output lines list the cluster units in vcluster 1 and are not always in priority order.

The default static weight for each cluster unit is 40. This means that sessions are distributed evenly among all cluster units. You can use the `set weight` command to change the static weights of cluster units to distribute sessions to cluster units depending on their priority in the cluster. The weight can be between 0 and 255. Increase the weight to increase the number of connections processed by the cluster unit with that priority.

You set the weight for each unit separately. For the example cluster of 5 FortiGate units you can set the weight for each unit as follows:

```
config system ha
   set mode a-a
   set schedule weight-roud-robin
   set weight 0 5
   set weight 1 10
   set weight 2 15
   set weight 3 20
   set weight 4 30
end
```

If you enter the `get` command to view the HA configuration the output for `weight` would be:

```
weight 5 10 15 20 30 40 40 40 40 40 40 40 40 40 40 40
```

This configuration has the following results if the output of the `get system ha status` command is that shown above:

- The first five connections are processed by the primary unit (host name head_office_cla, priority 0, weight 5). From the output of the
- The next 10 connections are processed by the first subordinate unit (host name head_office_clb, priority 1, weight 10)

- The next 15 connections are processed by the second subordinate unit (host name head_office_clc, priority 2, weight 15)
- The next 20 connections are processed by the third subordinate unit (host name head_office_cld, priority 3, weight 20)
- The next 30 connections are processed by the fourth subordinate unit (host name head_office_cle, priority 4, weight 30)

Dynamically optimizing weighted load balancing according to how busy cluster units are

In conjunction with using static weights to load balance sessions among cluster units you can configure a cluster to dynamically load balance sessions according to individual cluster unit CPU usage, memory usage, and number of HTTP, FTP, IMAP, POP3, SMTP, or NNTP proxy-based security proflie sessions. If any of these system loading indicators increases above configured thresholds, weighted load balancing dynamically sends fewer new sessions to the busy unit until it recovers.

High CPU or memory usage indicates that a unit is under increased load and may not be able to process more sessions. HTTP, FTP, IMAP, POP3, SMTP, or NNTP proxy use are also good indicators of how busy a cluster unit is, since processing high numbers of these proxy sessions can quickly reduce overall cluster unit performance.

For example, you can set a CPU usage high watermark threshold. When a cluster unit reaches this high watermark threshold fewer sessions are sent to it. With fewer sessions to process the cluster unit's CPU usage should fall back to the low watermark threshold. When the low watermark threshold is reached the cluster resumes normal load balancing of sessions to the cluster unit.

You can set individual high and low watermark thresholds and weights for CPU usage, memory usage, and for the number of HTTP, FTP, IMAP, POP3, SMTP, or NNTP proxy sessions.

The CPU usage, memory usage, and proxy weights determine how the cluster load balances sessions when a high watermark threshold is reached and also affect how the cluster load balances sessions when multiple cluster units reach different high watermark thresholds at the same time. For example, you might be less concerned about a cluster unit reaching the memory usage high watermark threshold than reaching the CPU usage high watermark threshold. If this is the case you can set the weight lower for memory usage. Then, if one cluster unit reaches the CPU usage high watermark threshold and a second cluster unit reaches the memory usage high watermark threshold the cluster will load balance more sessions to the cluster unit with high memory usage and fewer sessions to the cluster unit with high CPU usage. As a result, reaching the CPU usage high watermark will have a greater affect on how sessions are redistributed than reaching the memory usage high watermark.

When a high watermark threshold is reached, the corresponding weight is subtracted from the static weight of the cluster unit. The lower the weight the fewer the number of sessions that are load balanced to that unit. Subsequently when the low watermark threshold is reached, the static weight of the cluster unit returns to its configured value. For the weights to all be effective the weights assigned to the load indicators should usually be lower than or equal to the static weights assigned to the cluster units.

Use the following command to set thresholds and weights for CPU and memory usage and HTTP, FTP, IMAP, POP3, SMTP, or NNTP proxy sessions:

```
config system ha
   set mode a-a
   set schedule weight-round-robin
   set cpu-threshold <weight> <low> <high>
   set memory-threshold <weight> <low> <high>
   set http-proxy-threshold <weight> <low> <high>
   set ftp-proxy-threshold <weight> <low> <high>
   set imap-proxy-threshold <weight> <low> <high>
```

```
    set nntp-proxy-threshold <weight> <low> <high>
    set pop3-proxy-threshold <weight> <low> <high>
    set smtp-proxy-threshold <weight> <low> <high>
end
```

For each option, the weight range is 0 to 255 and the default weight is 5. The low and high watermarks are a percent (0 to 100). The default low and high watermarks are 0 which means they are disabled. The default configuration when weighted load balancing is enabled looks like the following:

```
config system ha
    set mode a-a
    set schedule weight-round-robin
    set cpu-threshold 5 0 0
    set memory-threshold 5 0 0
    set http-proxy-threshold 5 0 0
    set ftp-proxy-threshold 5 0 0
    set imap-proxy-threshold 5 0 0
    set nntp-proxy-threshold 5 0 0
    set pop3-proxy-threshold 5 0 0
    set smtp-proxy-threshold 5 0 0
end
```

When you first enable HA weighted load balancing, the weighted load balancing configuration is synchronized to all cluster units and each cluster unit has the default configuration shown above. Changes to the CPU, memory, HTTP, FTP, IMAP, NNTP, POP3, and SMTP proxy thresholds and low and high watermarks must be made for each cluster unit and are not synchronized to the other cluster units.

When you configure them, the high watermarks must be greater than their corresponding low watermarks.

For CPU and memory usage the low and high watermarks are compared with the percentage CPU and memory use of the cluster unit. For each of the proxies the high and low watermarks are compared to a number that represents percent of the max number of proxy sessions being used by a proxy. This number is calculated using the formula:

```
proxy usage = (current sessions * 100) / max sessions
```

where:

`current sessions` is the number of active sessions for the proxy type.

`max sessions` is the session limit for the proxy type. The session limit depends on the FortiGate unit and its configuration.

You can use the following command to display the maximum and current number of sessions for a proxy:

```
get test {ftpd | http | imap | nntp | pop3 | smtp} 4
```

You can use the following command to display the maximum number of sessions and the and current number of sessions for all of the proxies:

```
get test proxyworker 4
```

The command output includes lines similar to the following:

```
get test http 4
HTTP Common
Current Connections             5000/8032
```

In the example, `5000` is the current number of proxy connections being used by HTTP and 8032 is the maximum number of proxy sessions allowed. For this example the proxy usage would be:

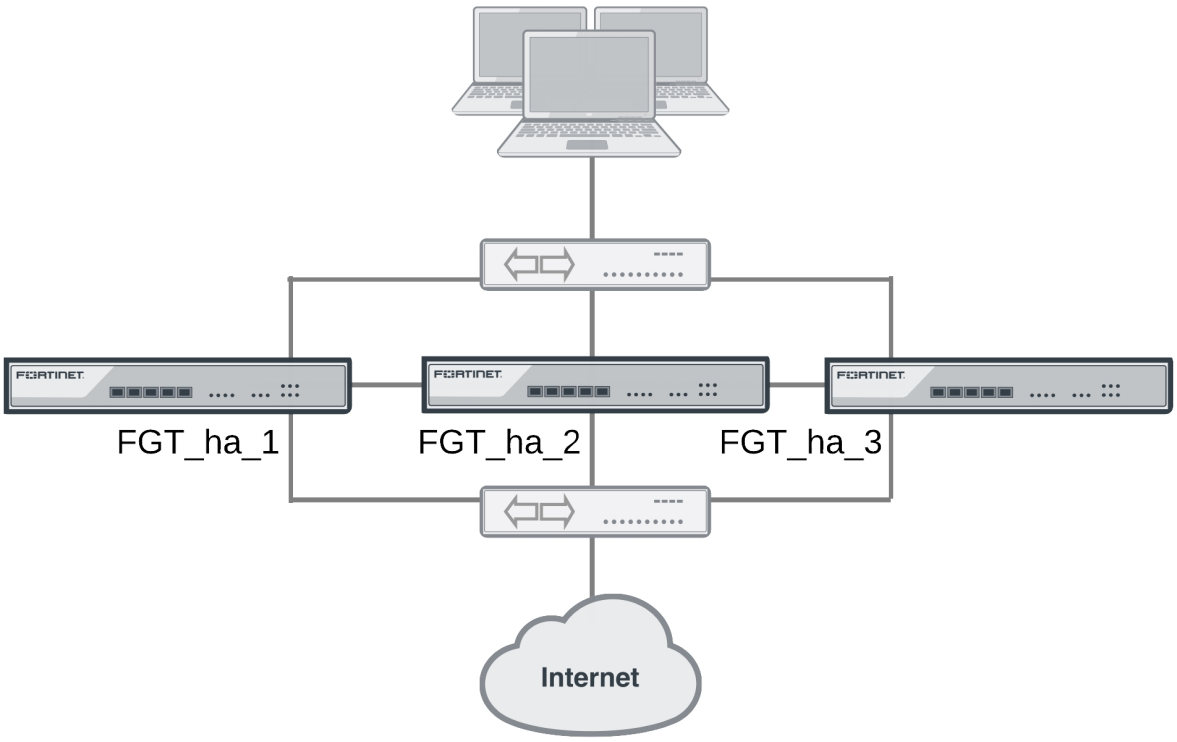
```
proxy usage = (5000 * 100) / 8032
```

```
proxy usage = 62%
```

Example weighted load balancing configuration

Consider a cluster of three FortiGate units with host names FGT_ha_1, FGT_ha_2, and FGT_ha_3 as shown below. This example describes how to configure weighted load balancing settings for CPU and memory usage for the cluster and then to configure HTTP and POP3 proxy weights to send most HTTP and POP3 proxy sessions to different cluster units.

Example HA weighted load balancing configuration



Connect to the cluster CLI and use the following command to set the CPU usage threshold weight to 30, low watermark to 60, and high watermark to 80. This command also sets the memory usage threshold weight to 10, low watermark to 60, and high watermark to 90.

```
config system ha
   set mode a-a
   set schedule weight-round-robin
   set cpu-threshold 30 60 80
   set memory-threshold 10 60 90
end
```

The static weights for the cluster units remain at the default values of 40. Since this command changes the mode to `a-a` and the schedule to `weight-round-robin` for the first time, the weight settings are synchronized to all cluster units.

As a result of this configuration, if the CPU usage of any cluster unit (for example, FGT_ha_1) reaches 80% the static weight for that cluster unit is reduced from 40 to 10 and only 10 of every 120 new sessions are load balanced to this cluster unit. If the memory usage of FGT_ha_1 also reaches 90% the static weight further reduces to 0 and no new sessions are load balanced to FGT_ha_1. Also, if the memory usage of 620_ha_2 reaches 90% the static weight of FGT_ha_2 reduces to 30 and 30 of every 120 new sessions are load balanced to FGT_ha_2.

Now that you have established the weight load balancing configuration for the entire cluster you can monitor the cluster to verify that processing gets distributed evenly to all cluster units. From the web-based manager you can go do **System > Config > HA > View HA Statistics** and see the CPU usage, active sessions, memory usage and other statistics for all of the cluster units. If you notice that one cluster unit is more or less busy than others you can adjust the dynamic weights separately for each cluster unit.

For example, in some active-active clusters the primary unit may tend to be busier than other cluster units because in addition to processing sessions the primary unit also receives all packets sent to the cluster and performs load balancing to distribute the sessions to other cluster units. To reduce the load on the primary unit you could reduce the CPU and memory usage high watermark thresholds for the primary unit so that fewer sessions are distributed to the primary unit. You could also reduce the primary unit's high watermark setting for the proxies to distribute more proxy sessions to other cluster units.

This would only be useful if you are using device priorities and override settings to make sure the same unit always becomes the primary unit. See An introduction to the FGCP on page 1270.

If the example cluster is configured for FGT_ha_2 to be the primary unit, connect to the FGT_ha_2's CLI and enter the following command to set CPU usage, memory usage, and proxy usage high watermark thresholds lower.

```
config system ha
   set cpu-threshold 30 60 70
   set memory-threshold 30 60 70
   set http-proxy-threshold 30 60 70
   set ftp-proxy-threshold 30 60 70
   set imap-proxy-threshold 30 60 70
   set nntp-proxy-threshold 30 60 70
   set pop3-proxy-threshold 30 60 70
   set smtp-proxy-threshold 30 60 70
end
```

As a result, when any of these factors reaches 70% on the primary unit, fewer sessions will be processed by the primary unit, preventing the number of sessions being processed from rising.

NAT/Route mode active-active cluster packet flow

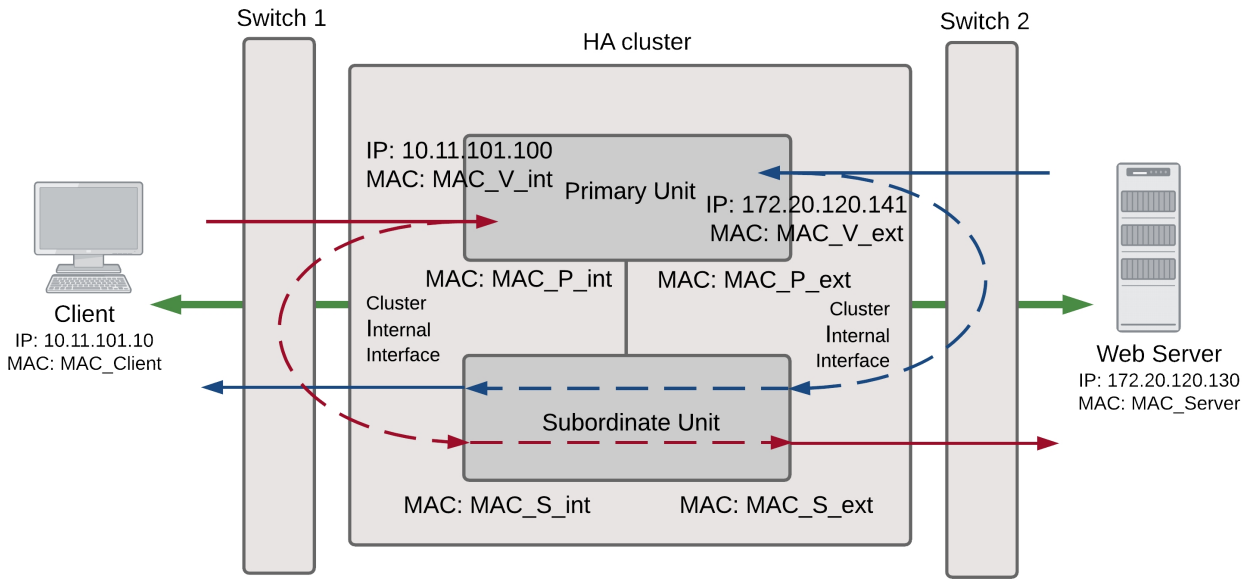
This section describes an example of how packets are load balanced and how failover occurs in an active-active HA cluster running in NAT/Route mode. In the example, the NAT/Route mode cluster acts as the internet firewall for a client computer's internal network. The client computer's default route points at the IP address of the cluster internal interface. The client connects to a web server on the Internet. Internet routing routes packets from the cluster external interface to the web server, and from the web server to the cluster external interface.

In NAT/Route mode, eight MAC addresses are involved in active-active communication between the client and the web server when the primary unit load balances packets to the subordinate unit:

- Internal virtual MAC address (MAC_V_int) assigned to the primary unit internal interface,
- External virtual MAC address (MAC_V_ext) assigned to the primary unit external interface,
- Client MAC address (MAC_Client),
- Server MAC address (MAC_Server),
- Primary unit original internal MAC address (MAC_P_int),
- Primary unit original external MAC address (MAC_P_ext),
- Subordinate unit internal MAC address (MAC_S_int),
- Subordinate unit external MAC address (MAC_S_ext).

In NAT/Route mode, the HA cluster works as a gateway when it responds to ARP requests. Therefore, the client and server only know the gateway MAC addresses. The client only knows the cluster internal virtual MAC address (MAC_V_int) and the server only knows the cluster external virtual MAC address (MAC_V_ext).

NAT/Route mode active-active packet flow



Packet flow from client to web server

1. The client computer requests a connection from 10.11.101.10 to 172.20.120.130.
2. The default route on the client computer recognizes 10.11.101.100 (the cluster IP address) as the gateway to the external network where the web server is located.
3. The client computer issues an ARP request to 10.11.101.100.
4. The primary unit intercepts the ARP request, and responds with the internal virtual MAC address (MAC_V_int) which corresponds to its IP address of 10.11.101.100.
5. The client's request packet reaches the primary unit internal interface.

	IP address	MAC address

Source	10.11.101.10	MAC_Client
Destination	172.20.120.130	MAC_V_int

6. The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit internal interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit internal interface.

	IP address	MAC address
Source	10.11.101.10	MAC_P_int
Destination	172.20.120.130	MAC_S_int

7. The subordinate unit recognizes that the packet has been forwarded from the primary unit and processes it.
8. The subordinate unit forwards the packet from its external interface to the web server.

	IP address	MAC address
Source	172.20.120.141	MAC_S_ext
Destination	172.20.120.130	MAC_Server

9. The primary unit forwards further packets in the same session to the subordinate unit.
10. Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

Packet flow from web server to client

1. When the web server responds to the client's packet, the cluster external interface IP address (172.20.120.141) is recognized as the gateway to the internal network.
2. The web server issues an ARP request to 172.20.120.141.
3. The primary unit intercepts the ARP request, and responds with the external virtual MAC address (MAC_V_ext) which corresponds its IP address of 172.20.120.141.
4. The web server then sends response packets to the primary unit external interface.

	IP address	MAC address
Source	172.20.120.130	MAC_Server
Destination	172.20.120.141	MAC_V_ext

5. The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit external interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit external interface.

	IP address	MAC address
Source	172.20.120.130	MAC_P_ext
Destination	172.20.120.141	MAC_S_ext

6. The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
7. The subordinate unit forwards the packet from its internal interface to the client.

	IP address	MAC address
Source	172.20.120.130	MAC_S_int
Destination	10.11.101.10	MAC_Client

8. The primary unit forwards further packets in the same session to the subordinate unit.
9. Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

When a failover occurs

The following steps are followed after a device or link failure of the primary unit causes a failover.

1. If the primary unit fails, the subordinate unit negotiates to become the primary unit.
2. The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC addresses.
   The new primary unit has the same IP addresses and MAC addresses as the failed primary unit.
3. The new primary units sends gratuitous ARP packets to the 10.10.101.0 network to associate its internal IP address with the internal virtual MAC address.
4. The new primary units sends gratuitous ARP packets to the 172.20.120.0 network to associate its external IP address with the external virtual MAC address.
5. Traffic sent to the cluster is now received and processed by the new primary unit.
   If there were more than two cluster units in the original cluster, the new primary unit would load balance packets to the remaining cluster members.

Transparent mode active-active cluster packet flow

This section describes an example of how packets are load balanced and how failover occurs in an active-active HA cluster running in Transparent mode. The cluster is installed on an internal network in front of a mail server and the client connects to the mail server through the Transparent mode cluster.

In Transparent mode, six MAC addresses are involved in active-active communication between a client and a server when the primary unit load balances packets to the subordinate unit:

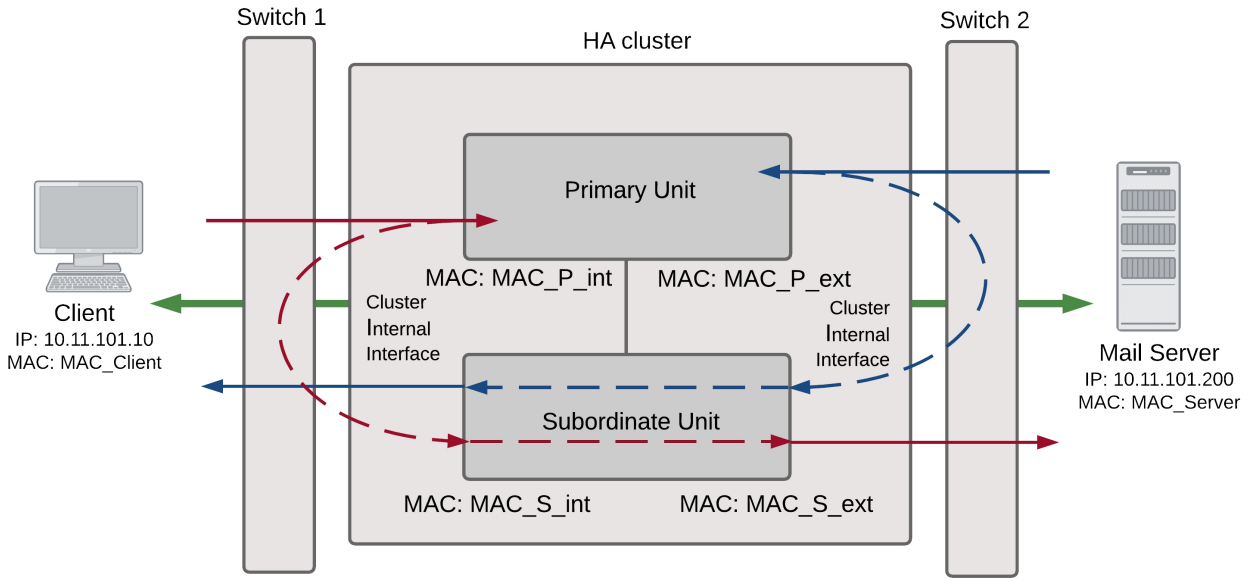
- Client MAC address (MAC_Client),
- Server MAC address (MAC_Server),
- Primary unit original internal MAC address (MAC_P_int),
- Primary unit original external MAC address (MAC_P_ext),
- Subordinate unit internal MAC address (MAC_S_int),
- Subordinate unit external MAC address (MAC_S_ext).

The HA virtual MAC addresses are not directly involved in communicate between the client and the server. The client computer sends packets to the mail server and the mail server sends responses. In both cases the packets are intercepted and load balanced among cluster members.

The cluster's presence on the network and its load balancing are transparent to the client and server computers. The primary unit sends gratuitous ARP packets to Switch 1 that associate all MAC addresses on the network

segment connected to the cluster external interface with the external virtual MAC address. The primary unit also sends gratuitous ARP packets to Switch 2 that associate all MAC addresses on the network segment connected to the cluster internal interface with the internal virtual MAC address. In both cases, this results in the switches sending packets to the primary unit interfaces.

Transparent mode active-active packet flow



Packet flow from client to mail server

1. The client computer requests a connection from 10.11.101.10 to 10.11.101.200.
2. The client computer issues an ARP request to 10.11.101.200.
3. The primary unit forwards the ARP request to the mail server.
4. The mail server responds with its MAC address (MAC_Server) which corresponds to its IP address of 10.11.101.200. The primary unit returns the ARP response to the client computer.
5. The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
Source	10.11.101.10	MAC_Client
Destination	10.11.101.200	MAC_Server

6. The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit internal interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit internal interface.

	IP address	MAC address

Source	10.11.101.10	MAC_P_int
Destination	10.11.101.200	MAC_S_int

7. The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
8. The subordinate unit forwards the packet from its external interface to the mail server.

	IP address	MAC address
Source	10.11.101.10	MAC_S_ext
Destination	10.11.101.200	MAC_Server

9. The primary unit forwards further packets in the same session to the subordinate unit.
10. Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

Packet flow from mail server to client

1. To respond to the client computer, the mail server issues an ARP request to 10.11.101.10.
2. The primary unit forwards the ARP request to the client computer.
3. The client computer responds with its MAC address (MAC_Client) which corresponds to its IP address of 10.11.101.10. The primary unit returns the ARP response to the mail server.
4. The mail server's response packet reaches the primary unit external interface.

	IP address	MAC address
Source	10.11.101.200	MAC_Server
Destination	10.11.101.10	MAC_Client

5. The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit external interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit external interface.

	IP address	MAC address
Source	10.11.101.200	MAC_P_ext
Destination	10.11.101.10	MAC_S_ext

6. The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
7. The subordinate unit forwards the packet from its internal interface to the client.

	IP address	MAC address
Source	10.11.101.200	MAC_S_int
Destination	10.11.101.10	MAC_Client

8. The primary unit forwards further packets in the same session to the subordinate unit.
9. Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

When a failover occurs

The following steps are followed after a device or link failure of the primary unit causes a failover.

1. If the primary unit fails the subordinate unit negotiates to become the primary unit.
2. The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.
3. The new primary units sends gratuitous ARP requests to switch 1 to associate its MAC address with the MAC addresses on the network segment connected to the external interface.
4. The new primary units sends gratuitous ARP requests to switch 2 to associate its MAC address with the MAC addresses on the network segment connected to the internal interface.
5. Traffic sent to the cluster is now received and processed by the new primary unit.

   If there were more than two cluster units in the original cluster, the new primary unit would load balance packets to the remaining cluster members.

HA with FortiGate-VM and third-party products

This chapter provides information about operating FortiOS VM cluster and operating FortiGate clusters with third party products such as layer-2 and layer-3 switches.

FortiGate-VM for VMware HA configuration

If you want to combine two or more FortiGate-VM instances into a FortiGate Clustering Protocol (FGSP) High Availability (HA) cluster the VMware server's virtual switches used to connect the heartbeat interfaces must operate in promiscuous mode. This permits HA heartbeat communication between the heartbeat interfaces. HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8893. The FGCP uses link-local IP4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

To enable promiscuous mode in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect heartbeat interfaces.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.

You must also set the virtual switches connected to other FortiGate interfaces to allow MAC address changes and to accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate interfaces and the same interfaces on the different VM instances in the cluster will have the same virtual MAC addresses.

To make the required changes in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect FortiGate VM interfaces.
4. Set **MAC Address Changes**to**Accept**.
5. Set **Forged Transmits** to **Accept**.

FortiGate VM for Hyper-V HA configuration

Promiscuous mode and support for MAC address spoofing is required for FortiGate-VM for Hyper-V to support FortiGate Clustering Protocol (FGCP) high availability (HA). By default the FortiGate-VM for Hyper-V has promiscuous mode enabled in the XML configuration file in the FortiGate-VM Hyper-V image. If you have problems with HA mode, confirm that this is still enabled.

In addition, because the FGCP applies virtual MAC addresses to FortiGate data interfaces and because these virtual MAC addresses mean that matching interfaces of different FortiGate-VM instances will have the same virtual MAC addresses you have to configure Hyper-V to allow MAC spoofing. But you should only enable MAC

spoofing for FortiGate-VM data interfaces. You should not enable MAC spoofing for FortiGate HA heartbeat interfaces.

With promiscuous mode enabled and the correct MAC spoofing settings you should be able to configure HA between two or more FortiGate-VM for Hyper-V instances.

Troubleshooting layer-2 switches

Issues may occur because of the way an HA cluster assigns MAC addresses to the primary unit. Two clusters with the same group ID cannot connect to the same switch and cannot be installed on the same network unless they are separated by a router.

Forwarding delay on layer 2 switches

You must ensure that if there is a switch between the FortiGate HA cluster and the network its is protecting and the switch has a forwarding delay (even if spanning tree is disabled) when one of its interfaces is activated then the forwarding delay should be set as low as possible. For example, some versions of Cisco IOS have a forwarding delay of 15 seconds even when spanning tree is disabled. If left at this default value then TCP session pickup can fail because traffic is not forwarded through the switch on HA failover.

Failover issues with layer-3 switches

After a failover, the new primary unit sends gratuitous ARP packets to refresh the MAC forwarding tables of the switches connected to the cluster. If the cluster is connected using layer-2 switches, the MAC forwarding tables (also called arp tables) are refreshed by the gratuitous ARP packets and the switches start directing packets to the new primary unit.

In some configurations that use layer-3 switches, after a failover, the layer-3 switches may not successfully re-direct traffic to the new primary unit. The possible reason for this is that the layer-3 switch might keep a table of IP addresses and interfaces and may not update this table for a relatively long time after the failover (the table is not updated by the gratuitous ARP packets). Until the table is updated, the layer-3 switch keeps forwarding packets to the now failed cluster unit. As a result, traffic stops and the cluster does not function.

As of the release date of this document, Fortinet has not developed a workaround for this problem. One possible solution would be to clear the forwarding table on the layer-3 switch.

The `config system ha link-failed-signal` command described in Updating MAC forwarding tables when a link failover occurs on page 1489 can be used to resolve link failover issues similar to those described here.

Changing spanning tree protocol settings for some switches

Configuration changes may be required when you are running an active-active HA cluster that is connected to a switch that operates using the spanning tree protocol. For example, the following spanning tree parameters may need to be changed:

Maximum Age	The time that a bridge stores the spanning tree bridge control data unit (BPDU) before discarding it. A maximum age of 20 seconds means it may take 20 seconds before the switch changes a port to the listening state.
Forward Delay	The time that a connected port stays in listening and learning state. A forward delay of 15 seconds assumes a maximum network size of seven bridge hops, a maximum of three lost BPDUs and a hello-interval of 2 seconds.

For an active-active HA cluster to be compatible with the spanning tree algorithm, the FGCP requires that the sum of maximum age and forward delay should be less than 20 seconds. The maximum age and forward delay settings are designed to prevent layer 2 loops. If there is no possibility of layer 2 loops in the network, you could reduce the forward delay to the minimum value.

For some Dell 3348 switches the default maximum age is 20 seconds and the default forward delay is 15 seconds. In this configuration the switch cannot work with a FortiGate HA cluster. However, the switch and cluster are compatible if the maximum age is reduced to 10 seconds and the forward delay is reduced to 5 seconds.

Spanning Tree protocol (STP)

Spanning tree protocol is an IEEE 802.1 standard link management protocol that for media access control bridges. STP uses the spanning tree algorithm to provide path redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. Loops can be created if there are more than route between two hosts. To control path redundancy, STP creates a tree that spans all of the switches in an extended network. Using the information in the tree, the STP can force redundant paths into a standby, or blocked, state. The result is that only one active path is available at a time between any two network devices (preventing looping). Redundant links are used as backups if the initial link should fail. Without spanning tree in place, it is possible that two connections may be simultaneously live, which could result in an endless loop of traffic on the network.

Bridge Protocol Data Unit (BPDU)

BPDUs are spanning tree data messages exchanged across switches within an extended network. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

Failover and attached network equipment

It normally takes a cluster approximately 6 seconds to complete a failover. However, the actual failover time may depend on how quickly the switches connected to the cluster interfaces accept the cluster MAC address update from the primary unit. If the switches do not recognize and accept the gratuitous ARP packets and update their MAC forwarding table, the failover time will increase.

Also, individual session failover depends on whether the cluster is operating in active-active or active-passive mode, and whether the content of the traffic is to be virus scanned. Depending on application behavior, it may take a TCP session a longer period of time (up to 30 seconds) to recover completely.

Ethertype conflicts with third-party switches

Some third-party network equipment may use packets with Ethertypes that are the same as the ethertypes used for HA heartbeat packets. For example, Cisco N5K/Nexus switches use Ethertype 0x8890 for some functions. When one of these switches receives Ethertype 0x8890 heartbeat packets from an attached cluster unit, the switch generates CRC errors and the packets are not forwarded. As a result, FortiGate units connected with these switches cannot form a cluster.

In some cases, if the heartbeat interfaces are connected and configured so regular traffic flows but heartbeat traffic is not forwarded, you can change the configuration of the switch that connects the HA heartbeat interfaces to allow level2 frames with Ethertypes 0x8890, 0x8891, and 0x8893 to pass.

You can also use the following CLI commands to change the Ethertypes of the HA heartbeat packets:

```
config system ha
   set ha-eth-type <ha_ethertype_4-digit_hex>
   set hc-eth-type <hc_ethertype_4-digit_hex>
   set l2ep-eth-type <l2ep_ethertype_4-digit_hex>
end
```

For more information, see Heartbeat packet Ethertypes on page 1461.

LACP, 802.3ad aggregation and third-party switches

If a cluster contains 802.3ad aggregated interfaces you should connect the cluster to switches that support configuring multiple Link Aggregation (LAG) groups.

The primary and subordinate unit interfaces have the same MAC address, so if you cannot configure multiple LAG groups a switch may place all interfaces with the same MAC address into the same LAG group; disrupting the operation of the cluster.

You can change the FortiGate configuration to prevent subordinate units from participating in LACP negotiation. For example, use the following command to do this for an aggregate interface named Port1_Port2:

```
config system interface
   edit Port1_Port2
      set lacp-ha-slave disable
   end
```

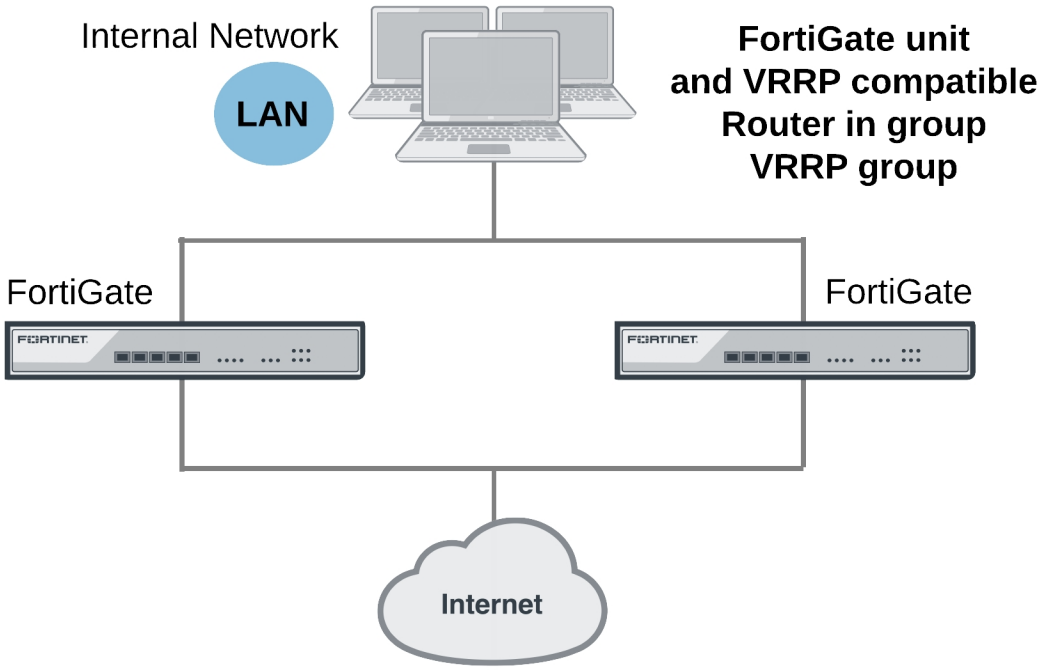
This configuration prevents the subordinate unit interfaces from sending or receiving packets. Resulting in the cluster not being able to operate in active-active mode. As well, failover may be slower because after a failover the new primary unit has to perform LACP negotiation before being able to process network traffic.

For more information, see Example: FGCP configuration examples and troubleshooting on page 1313.

VRRP

A Virtual Router Redundancy Protocol (VRRP) configuration can be used as a high availability solution to make sure that a network maintains connectivity with the Internet (or with other networks) even if the default router for the network fails. Using VRRP, if a router or a FortiGate unit fails all traffic to this router transparently fails over to another router or FortiGate unit that takes over the role of the router or FortiGate unit that failed. If the failed router or FortiGate unit is restored, it will once again take over processing traffic for the network. VRRP is described by RFC 3768.

Example VRRP configuration



To configure VRRP you create a VRRP group that contains two or more routers. Some or all of these routers can be FortiGate units. You can include different FortiGate models in the same VRRP group. The group members are configured to be the master router and one or more backup routers of the VRRP group. The network directs all traffic to the master's IP address and MAC address. If the master fails, VRRP dynamically shifts packet forwarding to a backup router. VRRP provides this redundancy without user intervention or additional configuration to any of the devices on the network.

The VRRP redundancy scheme means that devices on the network keep a single IP address for the default gateway and this IP address maps to a well-known virtual MAC address. If the VRRP master fails, one of the backup units becomes the new master and acquires virtual IP and MAC addresses that match the addresses of the master. The network then automatically directs all traffic to the backup unit. VRRP uses the broadcast capabilities of Ethernet networks. A long as one of the routers in a VRRP group is running, ARP requests for the

default gateway IP address always receive replies. Additionally, hosts can send packets outside their subnet without interruption.

FortiGate units support VRRP and can be quickly and easily integrated into a network that has already deployed a group of routers using VRRP. You can also create a new VRRP configuration consisting of a FortiGate unit acting as a VRRP master with one or more VRRP-compatible routers acting as backup routers. Some or all of those backup routers can be FortiGate units.

During normal operation the VRRP master unit sends VRRP advertisement messages to the backup units. A backup unit will not attempt to become a master unit while it is receiving these messages. When a FortiGate unit operating as a VRRP master fails, a backup unit takes its place and continues processing network traffic. The backup unit assumes the master unit has failed if it stops receiving the advertisement messages from the master unit. The backup unit with the highest priority becomes the new master unit after a short delay. During this delay the new master unit sends gratuitous ARPs to the network to map the virtual router IP address it its MAC address. As a result, all packets sent to the default route IP address are sent the new master unit. If the backup unit is a FortiGate unit, the network continues to benefit from FortiOS security features. If the backup unit is a router, after a failure traffic will continue to flow, but FortiOS security features will be unavailable until the FortiGate unit is back on line.

During a VRRP failover, as the backup unit starts to forward traffic it will not have session information for all of the failed over in-progress sessions. If the backup unit is operating as a normal FortiGate unit it will not be able to forward this traffic because of the lack of session information. To resolve this problem, immediately after a failover and for a short time as its taking over traffic processing, the backup unit operates with asymmetric routing enabled. This allows the backup unit to re-create all of the in-progress sessions and add them to the session table. While operating with asymmetric routing enabled, the backup unit cannot apply security functions. When the start-time ends the backup unit disables asymmetric routing and returns to normal operation including applying security functions.

Adding a VRRP virtual router to a FortiGate interface

Use the following command to add a VRRP virtual router to the port10 interface of a FortiGate unit. This VRRP virtual router has a virtual router ID of 200, uses IP address 10.31.101.200 and has a priority of 255. Since this is the highest priority this interface is configured to be the master of the VRRP group with ID number 200.

VRRP can be configured only on physical interfaces or VLAN interfaces. You cannot configure VRRP on hardware-switch interfaces where multiple physical interfaces are combined into a hardware switch interface.

```
config system interface
   edit port10
      config vrrp
         edit 200
            set vrip 10.31.101.200
            set priority 255
         end
   end
```

VRRP virtual MAC address

The VRRP virtual MAC address (or virtual router MAC address) is a shared MAC address adopted by the VRRP master. If the master fails the same virtual MAC master fails over to the new master. As a result, all packets for

VRRP routers can continue to use the same virtual MAC address. You must enable the VRRP virtual MAC address feature on all members of a VRRP group.

Each VRRP router is associated with its own virtual MAC address. The last part of the virtual MAC depends on the VRRP virtual router ID using the following format:

```
00-00-5E-00-01-<VRID_hex>
```

Where <VRID_hex> is the VRRP virtual router ID in hexadecimal format in internet standard bit-order. For more information about the format of the virtual MAC see RFC 3768.

Some examples:

- If the VRRP virtual router ID is 10 the virtual MAC would be 00-00-5E-00-01-0a.
- If the VRRP virtual router ID is 200 the virtual MAC would be 00-00-5E-00-01-c8.

The VRRP virtual MAC address feature is disabled by default. Wen you enable the feature on a FortiGate interface, all of the VRRP routers added to that interface use their own VRRP virtual MAC address. Each virtual MAC address will be different because each virtual router has its own ID.

Use the following command to enable the VRRP virtual MAC address on the port2 interface:

```
config system interface
   edit port2
      set vrrp-virtual-mac enable
   end
end
```

The port2 interface will now accept packets sent to the MAC addresses of the VRRP virtual routers added to this interface.

Using the VRRP virtual MAC address can improve network efficiency especially on large and complex LANs because when a failover occurs devices on the LAN do not have to learn a new MAC address for the new VRRP router.

If the VRRP virtual MAC address feature is disabled, the VRRP group uses the MAC address of the master. In the case of a FortiGate VRRP virtual router this is the MAC address of the FortiGate interface that the VRRP virtual routers are added to. If a master fails, when the new master takes over it sends gratuitous ARPs to associate the VRRP virtual router IP address with the MAC address of the new master (or the interface of the FortiGate unit that has become the new master). If the VRRP virtual MAC address is enabled the new master uses the same MAC address as the old master.

VRRP Groups

A VRRP group includes all the relevant VRRP IDs and tracks the VRRP status to force the status of all group members if a VRRP domain is changed from master to backup. VRRP groups are configured through the CLI. The VRRP group ID can be between 1 and 65535. Use the following command to add a VRRP group to the port20 interface that includes the virtual route identifiers 25, 50, 66 and 70 to VRRP group 10

```
config system interface
   edit port20
      config vrrp
         edit 25
            set vrgrp 10
         next
         edit 50
            set vrgrp 10
         next
         edit 66
            set vrgrp 10v
```

```
        next
        edit 70
           set vrgrp 10
    end
```

Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down.

Use the following command to configure a second destination IP (VRDST) to port14:

```
config system interface
   edit port14
      config vrrp
         edit 12
            set vrdst 10.10.10.20 10.20.20.10
      end
```

Configuring VRRP

To configure VRRP you must configure two or more FortiGate interfaces or routers with the same virtual router ID and IP address. Then these FortiGate units or routers can automatically join the same VRRP group. You must also assign priorities to each of the FortiGate units or routers in the VRRP group. One of the FortiGate units or routers must have the highest priority to become the master. The other FortiGate units or routers in the group are assigned lower priorities and become backup units. All of the units in the VRRP group should have different priorities. If the master unit fails, VRRP automatically fails over to the remaining unit in the group with the highest priority.

You configure VRRP from the FortiGate CLI by adding a VRRP virtual router to a FortiGate interface. You can add VRRP virtual routers to multiple FortiGate interfaces and you can add more than one virtual router to the same interface.

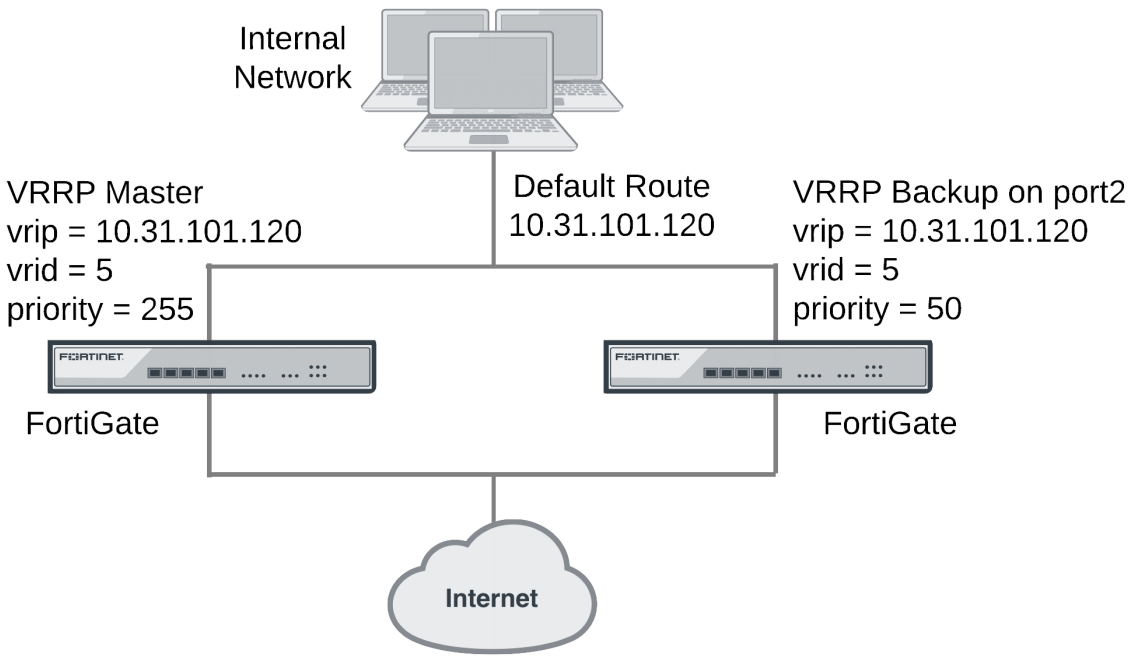
Example VRRP configuration: two FortiGate units in a VRRP group

This example includes a VRRP group consisting of two FortiGate units that connect an internal network to the Internet. As shown below, the internal network's default route is 10.31.101.120.

The FortiGate port2 interfaces connect to the internal network. A VRRP virtual router is added to each FortiGate unit's port2 interface. The virtual router IP address is 10.31.101.120 (the internal network's default route) and the virtual router's ID is 5. The VRRP priority of the master unit is set to 255 and the VRRP priority of the backup unit is 50. The port2 interface of each FortiGate unit should have an IP address that is different from the virtual router IP address and the port2 interface IP addresses should be different from each other.

This example also includes enabling the VRRP virtual MAC address on both FortiGate unit port2 interfaces so that the VRRP group uses the VRRP virtual MAC address.

Example VRRP configuration with two FortiGate units



To configure the FortiGate units for VRRP

1. Select one of the FortiGate units to be the VRRP master and the other to be the backup unit.
2. From the master unit's CLI, enter the following command to enable the VRRP virtual MAC address on the port2 interface and add the VRRP virtual router to the port2 interface:

```
config system interface
   edit port2
   set vrrp-virtual-mac enable
      config vrrp
         edit 5
            set vrip 10.31.101.120
            set priority 255
         end
   end
```

3. From the backup unit's CLI, enter the following command to enable the VRRP virtual MAC address on the port2 interface and add the VRRP virtual router to the port2 interface:

```
config system interface
   edit port2
      set vrrp-virtual-mac enable
      config vrrp
         edit 5
            set vrip 10.31.101.120
            set priority 50
         end
   end
```

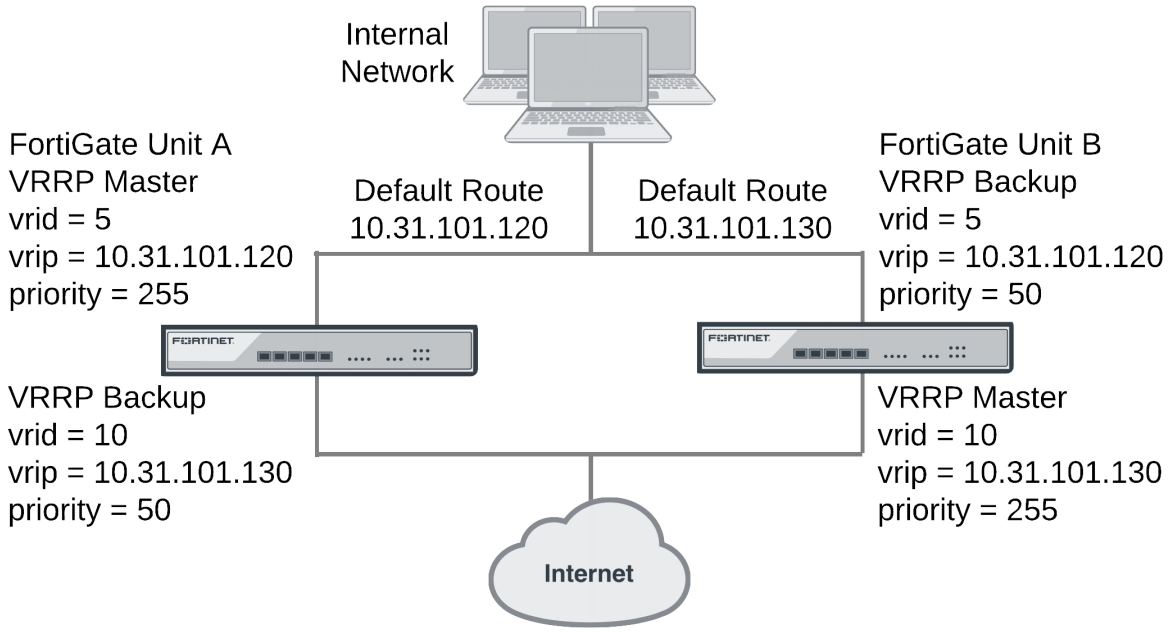
Example VRRP configuration: VRRP load balancing two FortiGate units and two VRRP groups

In this configuration two VRRP groups are involved. Each FortiGate unit participates in both of them. One FortiGate unit is the master of one group and the other FortiGate unit is the master of the other group. The network distributes traffic between two different default routes (10.31.101.120 and 10.31.101.130). One VRRP group is configured with one of the default route IP addresses and the other VRRP group get the other default route IP address. So during normal operation both FortiGate units are processing traffic and the VRRP groups are used to load balance the traffic between the two FortiGate units.

If one of the FortiGate units fails, the remaining FortiGate unit becomes the master of both VRRP groups. The network sends all traffic for both default routes to this FortiGate unit. The result is a configuration that under normal operation load balances traffic between two FortiGate units, but if one of the FortiGate units fails, all traffic fails over to the unit that is still operating.

This example also includes enabling the VRRP virtual MAC address on both FortiGate unit port2 interfaces so that the VRRP groups use their VRRP virtual MAC addresses.

Example VRRP configuration with two FortiGate units and two VRRP groups



To configure the FortiGate units

1. Log into the CLI of FortiGate unit A.
2. Enter the following command to enable the VRRP virtual MAC address feature and add the VRRP groups to the port2 interface of FortiGate unit A:

```
config system interface
   edit port2
      set vrrp-virtual-mac enable
```

```
      config vrrp
         edit 50 (32)
            set vrip 10.31.101.120
            set priority 255
         next
         edit 100 (64)
            set vrip 10.31.101.130
            set priority 50
         end
   end
```

3. Log into the CLI of FortiGate unit B.
4. Enter the following command to enable the VRRP virtual MAC address feature and add the VRRP groups to the port2 interface of FortiGate unit B:

```
config system interface
   edit port2
      set vrrp-virtual-mac enable
      config vrrp
         edit 50
            set vrip 10.31.101.120
            set priority 50
         next
         edit 100
            set vrip 10.31.101.130
            set priority 255
         end
   end
```

Optional VRRP configuration settings

In addition to the basic configuration settings, you can change to the VRRP configuration to:

- Adjust the virtual router advertisement message interval between 1 and 255 seconds using the `adv-interval` option.
- Adjust the startup time using the `start-time` option. The default start time is 3 seconds and the range is 1 to 255 seconds. The start time is the maximum time that the backup unit waits between receiving advertisement messages from the master unit. If the backup unit does not receive an advertisement message during this time it assumes the master has failed and becomes the new master unit. In some cases the advertisement messages may be delayed. For example, some switches with spanning tree enabled may delay some of the advertisement message packets. If you find that backup units are attempting to become master units without the master unit failing, you can extend the start time to make sure the backup units wait long enough for the advertisement messages.
- Enable or disable individual virtual router configurations using the `status` option. Normally virtual router configurations are enabled but you can temporarily disable one if its not required.
- Enable or disable preempt mode using the `preempt` option. In preempt mode a higher priority backup unit can preempt a lower priority master unit. This can happen if a master has failed, a backup unit has become the master unit, and the failed master is restarted. Since the restarted unit will have a higher priority, if preempt mode is enabled the restarted unit will replace the current master unit. Preempt mode is enabled by default.
- Monitor the route to a destination IP address using the `vrdst` option.

FortiGate Session Life Support Protocol (FGSP)

In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two identical FortiGate units can be integrated into the load balancing configuration using the FortiGate Session Life Support Protocol (FGSP). The external load balancers or routers can distribute sessions among the FortiGate units and the FGSP performs session synchronization of IPv4 and IPv6 TCP, UDP, ICMP, expectation, and NAT sessions to keep the session tables of both FortiGate units synchronized.

You can use the `config system session-sync` command to configure the FortiGate Session Life Support Protocol (FGSP) (previously called TCP session synchronization or standalone session synchronization) between two FortiGate units. The two FortiGate units must be the same model. The FGSP synchronizes both IPv4 and IPv6 TCP, UDP, ICMP, expectation, and NAT sessions. You can use this feature with external routers or load balancers configured to distribute or load balance sessions between two peer FortiGate units. If one of the peers fails, session failover occurs and active sessions fail over to the peer that is still operating. This failover occurs without any loss of data. As well, the external routers or load balancers will detect the failover and re-distribute all sessions to the peer that is still operating.

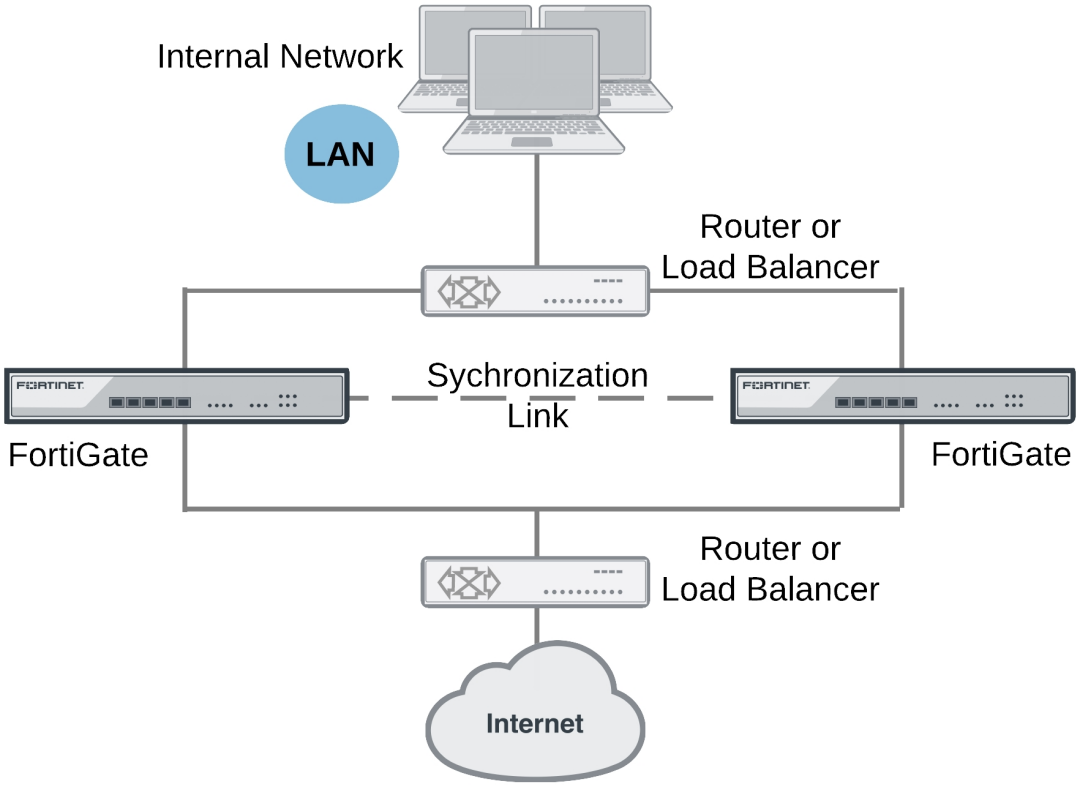
In previous versions of FortiOS the FGSP was called TCP session synchronization or standalone session synchronization. However, the FGSP has been expanded to include configuration synchronization and session synchronization of connectionless sessions, expectation sessions, and NAT sessions.

You cannot configure FGSP HA when FGCP HA is enabled. However FGSP HA is compatible with VRRP.

FGSP or standalone session synchronization is not supported if the FortiGate units are running different firmware versions.

The FGSP can be used instead of FGCP HA to provide **session synchronization** between two peer FortiGate units. If the external load balancers direct all sessions to one peer the affect is similar to active-passive FGCP HA. If external load balancers or routers load balance traffic to both peers, the effect is similar to active-active FGCP HA. The load balancers should be configured so that all of the packets for any given session are processed by the same peer. This includes return packets.

FGSP HA



By default, FGSP synchronizes all IPv4 and IPv6 TCP sessions and also synchronizes the configuration of the FortiGate units.

You can optionally enable session pickup to synchronize connectionless (UDP and ICMP) sessions, expectation sessions, and NAT sessions. If you do not enable session pickup, the FGSP does not share session tables for the particular session type and sessions do not resume after a failover. All sessions that are interrupted by the failover and must be re-established at the application level. Many protocols can successfully restart sessions with little, or no, loss of data. Others may not recover easily. Enable session pickup for sessions that may be difficult to reestablish. Since session pickup requires FortiGate resources, only enable this feature for sessions that you need to have synchronized.

You can also optionally add filters to control which sessions are synchronized. You can add filters to only synchronize packets from specified source and destination addresses, specified source and destination interfaces, and specified services.

Load balancing and session failover is done by external routers or load balancers instead of by the FGSP. The FortiGate units just perform session synchronization to support session failover.

Synchronizing the configuration

The FGSP also includes configuration synchronization, allowing you to make configuration changes once for both FortiGate units instead of requiring you to make duplicate configuration changes on each FortiGate unit. Settings that identify the FortiGate unit to the network, for example, interface IP addresses and BGP neighbor settings, are not synchronized so each FortiGate unit maintains its identity on the network.

By default configuration synchronization is disabled. You can use the following command to enable it.

```
config system ha
   set standalone-config-sync enable
end
```

Synchronizing UDP and ICMP (connectionless) sessions

In many configurations, due to their non-stateful nature, UDP and ICMP sessions don't need to be synchronized to naturally failover. However, if its required you can configure the FGSP to synchronize UDP and ICMP sessions by entering the following command:

```
config system ha
   set session-pickup enable
   set session-pickup-connectionless enable
end
```

Synchronizing NAT sessions

By default, NAT session are not synchronized. However, the FGSP can synchronize NAT session if you enter the following command:

```
config system ha
   set session-pickup enable
   set session-pickup-nat enable
end
```

However, if you want NAT sessions to resume after a failover you should not configure NAT to use the destination interface IP address since the FGSP FortiGate units have different IP addresses. With this configuration, after a failover all sessions that include the IP addresses of interfaces on the failed FortiGate unit will have nowhere to go since the IP addresses of the failed FortiGate unit will no longer be on the network.

Instead, in an FGSP configuration, if you want NAT sessions to failover you should use IP pools with the type set to overload (which is the default IP pool type). For example:

```
config firewall ippool
   edit FGSP-pool
      set type overload
      set startip 172.20.120.10
      set endip 172.20.120.20
   end
```

Then when you configure NAT firewall policies, turn on NAT and select to use dynamic IP pool and select the IP Pool that you added. Add the same IP pools and firewall policies to both FortiGate units.

Synchronizing asymmetric sessions

By default, asymmetric sessions are not synchronized. Normally, session synchronization cannot be asymmetric because it is stateful. So all of the packets of a given session must be processed on the same peer. This includes return packets.

However, if you have an asymmetric routing configuration, you can enter the following command to synchronize asymmetric sessions by dynamically detecting asymmetric sessions and disabling anti-reply for these sessions.

```
config system ha
   set session-pickup enable
   set session-pickup-expectation enable
end
```

The FGSP enforces firewall policies for asymmetric traffic, including cases where the TCP 3-way handshake is split between two FortiGates. For example, FGT-A receives the TCP-SYN, FGT-B receives the TCP-SYN-ACK, and FGT-A receives the TCP-ACK. Under normal conditions a firewall will drop this connection since the 3-way handshake was not seen by the same firewall. However two FortiGates with FGSP configured will be able to properly pass this traffic since the firewall sessions are synchronized.

This asymmetric function can also work with connectionless UDP and ICMP traffic. If traffic will be highly asymmetric, as described above, the following command must be enabled on both FortiGates.

```
config system ha
   set session-pickup enable
   set session-pickup-connectionless enable
end
```

Synchronizing asymmetric traffic can be very useful in situations where multiple Internet connections from different ISPs are spread across two FortiGates. Since it is typically not possible to guarantee Internet bound traffic leaving via an ISP will return using the exact same ISP, the FGSP provides critical firewall functions in this situation.

Asymmetric sessions may not be synchronized in low latency networks if the reply packet is received before the peer has received the session synchronization packet. This limitation usually only occurs in low latency networks.

The FGSP also has applications in virtualized computing environments where virtualized hosts move between data centers. The firewall session synchronization features of FGSP allow for more flexibility than in traditional firewalling functions.

Synchronizing expectation sessions

FortiOS session helpers keep track of the communication of Layer-7 protocols such as FTP and SIP that have control sessions and expectation sessions. Usually the control sessions establish the link between server and client and negotiate the ports and protocols that will be used for data communications. The session helpers then create expectation sessions through the FortiGate for the ports and protocols negotiated by the control session.

The expectation sessions are usually the sessions that actually communicate data. For FTP, the expectation sessions transmit files being uploaded or downloaded. For SIP, the expectation sessions transmit voice and video data. Expectation sessions usually have a timeout value of 30 seconds. If the communication from the server is not initiated within 30 seconds the expectation session times out and traffic will be denied.

By default the FGSP does not synchronize expectation sessions and if a failover occurs the sessions will have to be restarted.

If you want to synchronize expectation sessions so that they will continue after a failover you can enter the following command on both FortiGates to synchronize them:

```
config system ha
   set session-pickup enable
   set session-pickup-expectation enable
end
```

Security profile flow-based inspection and asymmetric traffic

Security profile inspection (flow or proxy based) for a session is not expected to work properly if the traffic in the session is balanced across more than one FortiGate in either direction. Flow-based inspection should be used in

FGSP deployments.

For an environment where traffic is symmetric, security profile inspection can be used with the following limitations:

- No session synchronization for the sessions inspected using proxy-based inspection. Sessions will drop and need to be reestablished after data path failover.
- Sessions with flow-based inspection will failover; however, inspection of failed over sessions after the failover may not work.

A single FortiGate must see both the request and reply traffic for security profile inspection to function correctly. For environments where asymmetric traffic is expected, security profile inspection should not be used.

Notes and limitations

FGSP HA has the following limitations:

- The FGSP is a global configuration option. As a result you can only add one service to a filter configuration. You cannot add custom services or service groups even if virtual domains are not enabled.
- You can only add one filter configuration to a given FGSP configuration. However, you can add multiple filters by adding multiple identical FGSP configurations, each one with a different filter configuration.
- Sessions accepted by security policies with security profiles configured are not synchronized.
- FGSP HA is configured from the CLI.
- FGSP HA is available for FortiGate units or virtual domains operating in NAT/Route or Transparent mode. NAT sessions are not synchronized in either mode (unless NAT synchronization is enabled as described in Synchronizing NAT sessions on page 1538). In NAT/Route mode, only sessions for route mode security policies are synchronized. In Transparent mode, only sessions for normal Transparent mode policies are synchronized.
- FGSP HA is supported for traffic on physical interfaces, VLAN interfaces, zones, aggregate interfaces, and NPx (NP4, NP6 etc.) accelerated interfaces. The FGSP has not been tested for inter-vdom links, between HA clusters, and for redundant interfaces.
- The names of the matching interfaces, including VLAN interfaces, aggregate interfaces and so on, must be the same on both peers.

Configuring FGSP HA

You configure FGSP HA separately for each virtual domain to be synchronized. If virtual domain configuration is not enabled, you configure FGSP HA for the root virtual domain. When virtual domain configuration is enabled and you have added virtual domains you configure FGSP HA for each virtual domain to be synchronized. You don't have to synchronize all virtual domains.

You must configure FGSP HA and network settings on both peers. Once you establish the initial configuration, the configurations of both FortiGate units are synchronized so when you change the configuration of one, the changes are synchronized to the other.

On each FortiGate unit, configuring FGSP HA consists of selecting the virtual domains to be synchronized using the `syncvd` field, selecting the virtual domain on the other peer that receives the synchronization packets using the `peervd` field, and setting the IP address of the interface in the peer unit that receives the synchronization packets using the `peerip` field. The interface with the `peerip` must be in the `peervd` virtual domain.

The `syncvd` and `peervd` settings must be the same on both peers. However, the `peerip` settings will be different because the `peerip` setting on the first peer includes the IP address of an interface on the second peer. And the `peerip` setting on the second peer includes the IP address of an interface on the first peer.

For FGSP HA to work properly all synchronized virtual domains must be added to both peers. The names of the matching interfaces in each virtual domain must also be the same; this includes the names of matching VLAN interfaces. Note that the index numbers of the matching interfaces and VLAN interfaces can be different. Also the VLAN IDs of the matching VLAN interfaces can be different.

Configuring the session synchronization link

When FGSP HA is operating, the peers share session information over an Ethernet link between the peers similar to an HA heartbeat link. Usually you would use the same interface on each peer for session synchronization. You should connect the session synchronization interfaces directly without using a switch or other networking equipment. For FortiGate-5000 systems you can use a backplane interface as the session synchronization link.

You can use different interfaces on each peer for session synchronization links. Also, if you have multiple sessions synchronization configurations, you can have multiple links between the peers. In fact if you are synchronizing a lot of sessions, you may want to configure and connect multiple session synchronization links to distribute session synchronization traffic to these multiple links.

You cannot configure backup session synchronization links. Each configuration only includes one session synchronization link.

The session synchronization link should always be maintained. If session synchronization communication is interrupted and a failure occurs, sessions will not failover and data could be lost.

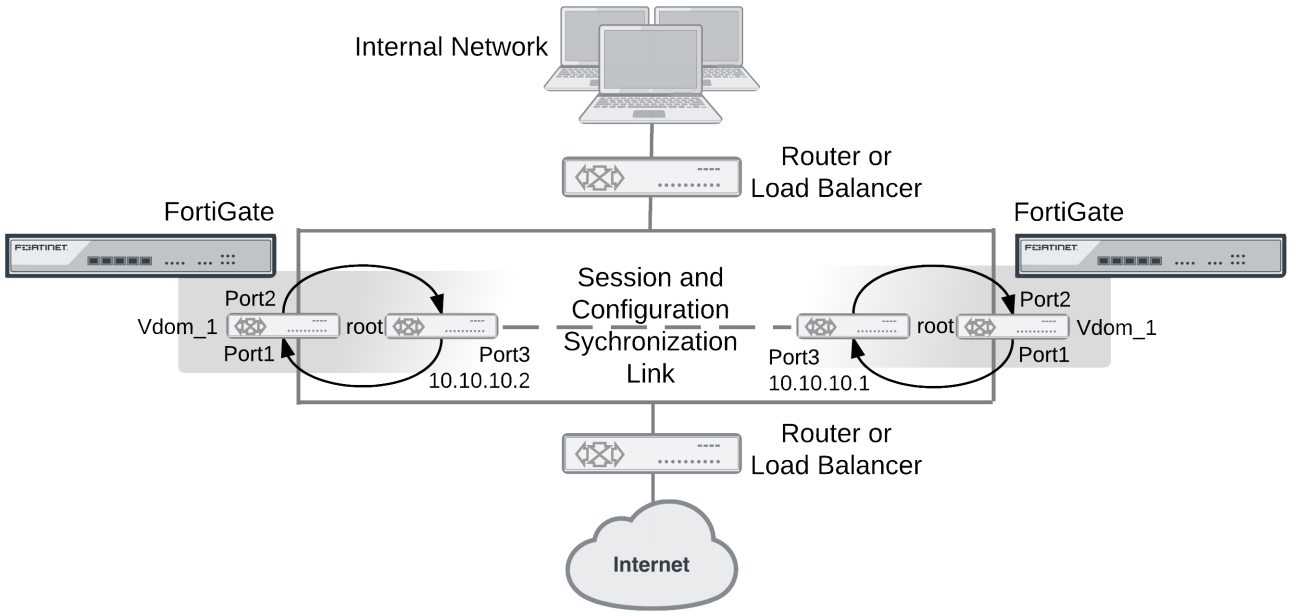
Session synchronization traffic can use a considerable amount of network bandwidth. If possible, session synchronization link interfaces should only be used for session synchronization traffic and not for data traffic.

Basic example configuration

The following configuration example shows how to configure basic FGSP HA for the two peer FortiGate units shown below. The host names of peers are peer_1 and peer_2. Both peers are configured with two virtual domains: root and vdom_1. All sessions processed by vdom_1 are synchronized. The synchronization link interface is port3 which is in the root virtual domain. The IP address of port3 on peer_1 is 10.10.10.1. The IP address of port3 on peer_2 is 10.10.10.2.

Also on both peers, port1 and port2 are added to vdom_1. On peer_1 the IP address of port1 is set to 192.168.20.1 and the IP address of port2 is set to 172.110.20.1. On peer_2 the IP address of port1 is set to 192.168.20.2 and the IP address of port2 is set to 172.110.20.2.

Example FGSP HA network configuration



To configure FGSP HA

1. Configure the load balancer or router to send all sessions to peer_1.
2. Configure the load balancer or router to send all traffic to peer_2 if peer_1 fails.
3. Use normal FortiGate configuration steps on peer_1:
   - Enable virtual domain configuration.
   - Add the vdom_1 virtual domain.
   - Add port1 and port2 to the vdom_1 virtual domain and configure these interfaces.
   - Set the IP address of port1 to 192.168.20.1.
   - Set the IP address of port2 to 172.110.20.1.
   - Set the IP address of port3 to 10.10.10.1.
   - Add route mode security policies between port1 and port2 to vdom_1.
4. Enter the following commands to configure session synchronization for peer_1

```
config system session-sync
   edit 1
      set peerip 10.10.10.2
      set peervd root
      set syncvd vdom_1
end
```

5. Use normal FortiGate configuration steps on peer_2:
   - Enable virtual domain configuration.
   - Add the vdom_1 virtual domain.
   - Add port1 and port2 to the vdom_1 virtual domain and configure these interfaces.
   - Set the IP address of port1 to 192.168.20.2.
   - Set the IP address of port2 to 172.110.20.2.
   - Set the IP address of port3 to 10.10.10.1.
   - Add route mode security policies between port1 and port2 to vdom_1.
6. Enter the following command to configure session synchronization for peer_1

```
config system session-sync
   edit 1
      set peerip 10.10.10.1
      set peervd root
      set syncvd vdom_1
end
```

Now that the FortiGate units are connected and configured their configurations are synchronized, so when you make a configuration change on one FortiGate unit it is synchronized to the other one.

To add filters

You can add a filter to this basic configuration if you only want to synchronize some TCP sessions. For example you can enter the following command to add a filter so that only HTTP sessions are synchronized:

```
config system session-sync
   edit 1
      config filter
         set service HTTP
      end
end
```

You can also add a filter to control the source and destination addresses of the IPv4 packets that are synchronized. For example you can enter the following command to add a filter so that only sessions with source addresses in the range 10.10.10.100 to 10.10.10.200 are synchronized.

```
config system session-sync
   edit 1
      config filter
         set srcaddr 10.10.10.100 10.10.10.200
      end
end
```

You can also add a filter to control the source and destination addresses of the IPv6 packets that are synchronized. For example you can enter the following command to add a filter so that only sessions with destination addresses in the range 2001:db8:0:2::/64 are synchronized.

```
config system session-sync
   edit 1
      config filter
         set dstaddr6 2001:db8:0:2::/64
      end
end
```

To synchronize UDP and ICMP sessions

You enter the following command to add synchronization of UDP and ICMP sessions to this configuration:

```
config system ha
   set session-pickup enable
   set session-pickup-connectionless enable
end
```

To synchronize the configuration

Enter the following command to enable configuration synchronization.

```
config system ha
   set standalone-config-sync enable
end
```

Verifying FGSP configuration and synchronization

You can use the following diagnose commands to verify that the FGSP and its synchronization functions are operating correctly.

FGSP configuration summary and status

Enter the following command to display a summary of the FGSP configuration and synchronization status:

```
diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_redir=0, sync_nat=1.
sync: create=12:0, update=0, delete=0:0, query=14
recv: create=14:0, update=0, delete=0:0, query=12
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
nCfg_sess_sync_num=5, mtu=16000
sync_filter:
1: vd=0, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0,
```

`sync_started=1` shows that synchronization is working. If this is set to 0 then something is not correct with session synchronization and synchronization has not been able to start because of it.

`sync_tcp=1`, `sync_others=1`, `sync_expectation=1`, and `sync_nat=1` show that the FGSP has been configured to synchronize TCP, connectionless, asymmetric, and NAT sessions.

`sync: create=12:0` and `recv: create=14:0` show that this FortiGate has synchronized 12 sessions to its peer and has received 14 sessions from its peer.

`sync_filter` shows the configured FGSP filter. In this case no filter has been created so all sessions are synchronized.

`vd=0` indicates that root VDOM sessions are synchronized.

Verifying that sessions are synchronized

Enter the command `diagnose sys session list` to display information about the sessions being processed by the FortiGate. In the command output look for sessions that should be synchronized and make sure they contain output lines that include `synced` (for example, `state=log may_dirty ndr synced`) to confirm that they are being synchronized by the FGSP.

```
diagnose sys session list
session info: proto=6 proto_state=05 duration=469 expire=0 timeout=3600
flags=00000000 sockflag=00000000 sockport=21 av_idx=0 use=4
origin-shaper=
```

```
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=log may_dirty ndr synced
statistic(bytes/packets/allow_err): org=544/9/1 reply=621/7/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=46->45/45->46
gwy=10.2.2.1/10.1.1.1
hook=pre dir=org act=noop 192.168.1.50:45327->172.16.1.100:21(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.1.100:21->192.168.1.50:45327(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00002deb tos=ff/ff ips_view=1 app_list=2000 app=16427
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=192.168.1.50, bps=633
```

Configuring FRUP

The FortiGate Redundant UTM Protocol (FRUP) provides similar redundancy to FGCP full mesh HA in a single unified design that includes redundant switching and routing. FRUP is available on the FortiGate-100D and will be expanded to other models in future releases.

A FRUP cluster consists of 2 (and only 2) identical FortiGate-100D units that have dual redundant links to all connected devices and networks and can include redundant FortiAP units. Connections to the Internet normally use the wan1 and wan2 interfaces for redundant connections. Connections to internal networks and servers use redundant connections to FortiGate-100D switch ports. FRUP uses the FortiGate-100D switch ports for full mesh HA instead of external redundant switches.

Each device or network has a default active connection to one of the FortiGate units and a default backup connection to the other. Ideally, the default active and backup connections should balance traffic between the FortiGate units in the cluster so that both FortiGate units are processing the same amount of traffic.

FRUP uses virtual IPs and virtual MACs so that when a failover occurs, network devices do not have to learn new IP or MAC addresses. FRUP also synchronizes the configuration between the units in the cluster.

Use the following CLI command on both FortiGate-100D units to configure FRUP.

```
config system ha
   set hbdev "ha1" 50 "ha2" 100
   set override disable
   set priority 128
   set frup enable
      config frup-settings
         set active-interface "wan2"
         set active-switch-port 14
         set backup-interface "wan1"
      end
end
```

Both units must have the same heartbeat device configuration and have FRUP enabled to form a FRUP cluster. Active interface and switch ports must be complementary according to your configuration (see the following example).

FRUP and the mode of the FortiGate hardware switch

FRUP is only available when the FortiGate's internal hardware switch is configured to operate as a switch. You can determine the current internal switch mode using the following command:

```
get system status
...
Internal Switch Mode: switch
...
```

If `Internal Switch Mode` is set to `switch` the hardware switch is operating in the correct mode and you can configure FRUP. If Internal Switch Mode is set to `interface` or `hub` you need to enter the following command to set it to hardware switch mode:

```
config system global
   set internal-switch-mode switch
end
```

Before you can set the switch to hardware switch mode you need to remove all configuration settings that will be affected by this change. This includes firewall policies and DHCP servers. Also, if you have configured a software switch you must remove it. You can use the following command:

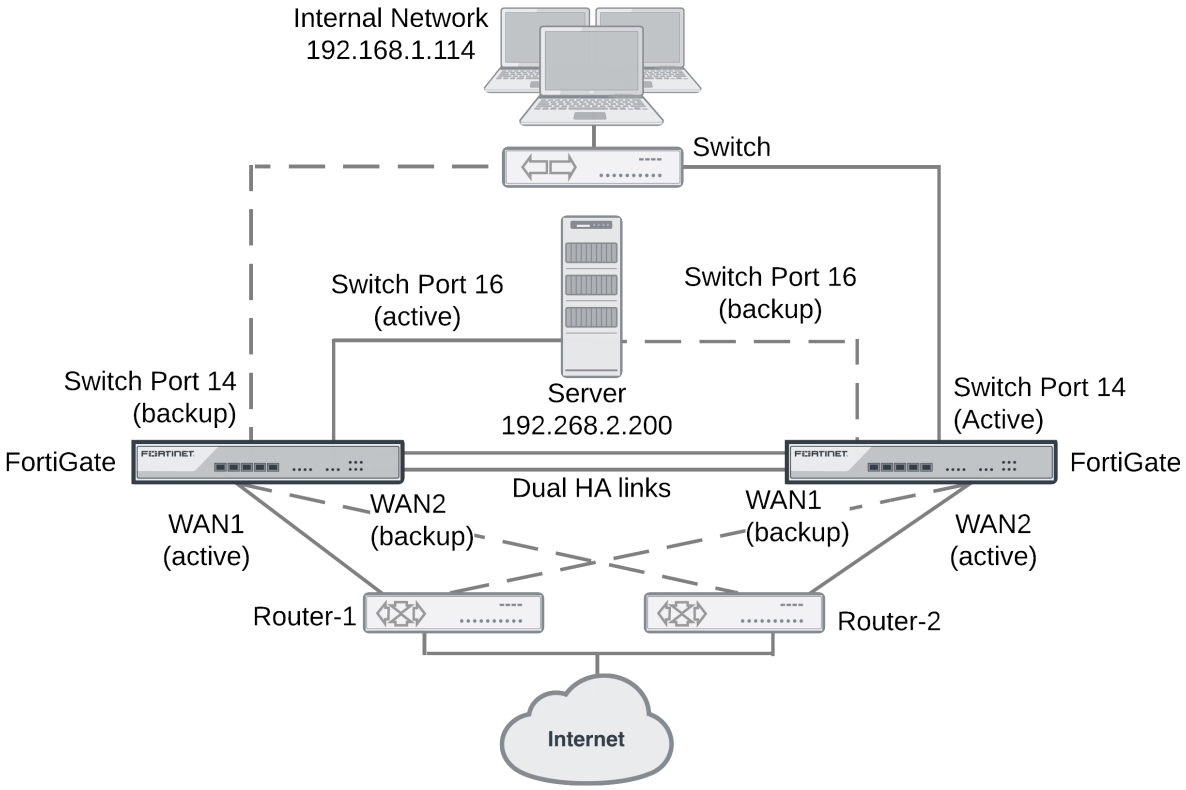
```
config system virtual-switch
   purge
end
```

FRUP configuration example

This example includes the following:

- Two FortiGate-100D units (FGT-A and FGT-B)
- HA1 and HA2 for redundant HA heartbeat connectivity between FGT-1 and FGT-2
- Dual gateways (router1 and router2):
  - FGT-A has an active connection from WAN1 to router-1 and a backup connection from WAN2 to router-2
  - FGT-B has an active connection from WAN2 to router-2 and a backup connection from WAN1 to router-1
- Dual connections to the internal network and an internal server:
  - FGT-A has an active connection to an internal server using switch port 16 and a backup connection to the internal network using switch port 14
  - FGT-B has a backup connection to an internal server using switch port 16 and an active connection to the internal network using switch port 14
- FortiGate interfaces use virtual IP addresses and pseudo-MAC physical addresses, all devices continue to send to the same IP/Mac and don't need to re-learn after a failover
- Both FortiGate units will handle and process traffic
- Backup links are normally administratively down
- Sessions and the FortiGate configuration are synchronized between the cluster units

Example FRUP configuration



Configuring FGT-A

Change the host name to FGT-A. Set up FGT-A with dual redundant internet links using WAN1 and WAN2. Set WAN1 and WAN2 interfaces to use static addressing and set both static routes to same priority and distance.

From CLI enter the following command:

```
config system ha
   set hbdev "ha1" 50 "ha2" 100
   set override disable
   set priority 255
   set frup enable
      config frup-settings
         set active-interface "wan1"
         set active-switch-port 16
         set backup-interface "wan2"
      end
   end
```

Configuring FGT-B

Use the same firmware version as FGT-A and set the FortiGate unit to factory defaults. Change the host name to FGT-B.

From CLI enter the following command:

```
config system ha
   set hbdev "ha1" 50 "ha2" 100
   set override disable
   set priority 128
   set frup enable
      config frup-settings
         set active-interface "wan2"
         set active-switch-port 14
         set backup-interface "wan1"
      end
   end
```

Connecting, testing and operating the FRUP cluster

Connect to the FortiGate-100D units to the network as shown in the diagram and power them on. The FortiGate-100D units should find each other and form a cluster.

Traffic from the server (IP: 192.168.1.200) connected to port16 should pass through FGT-A (since port16 is the active-switch-port in FGT-A) and to the Internet using WAN1 (since WAN1 is the active-interface in FGT-A).

Run a sniffer on both FortiGate units using the following command:

```
diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
```

Then run a ping to 4.2.2.2 from the server. The sniffer should show results similar to the following:

```
FGT-A # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
0.231160 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
0.231202 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
0.231209 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
1.198520 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
1.198555 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
1.222569 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
1.222589 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
1.222595 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
2.199916 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
2.199952 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
2.232998 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
2.233017 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
2.233023 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
3.201347 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
3.201385 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
3.235406 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
3.235425 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
3.235430 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply

18 packets received by filter
0 packets dropped by kernel

FGT-A #
```

Traffic initiating from a host on the internal network (for example, IP: 192.168.1.114) connected to port14 should flow through FGT-B (since port14 is the active-switch-port in FGT-B) to the Internet using WAN2 (since WAN2 is FGT-B's active interface).

Run the same sniffer on both FortiGate units and then run a ping to 74.125.226.1 from the internal network. The sniffer should show results similar to the following:

```
FGT-B $ diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
1.887458 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
1.887488 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
1.887492 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
1.898137 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
1.898153 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
1.898159 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
2.885644 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
2.885682 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
2.885687 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
2.896175 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
2.896194 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
2.896201 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
3.884046 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
3.884091 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
3.884096 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
3.894192 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
3.894213 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
3.894220 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply

18 packets received by filter
0 packets dropped by kernel

FGT-B $
```

Shutdown FGT-A.

Traffic from the internal network should be handled by FGT-B using WAN1 and WAN2 interfaces:

```
FGT-B # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
0.954086 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
0.954226 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
0.968696 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
0.968780 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
0.968796 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
1.166934 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
1.166960 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
1.166966 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
1.177525 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
1.177541 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
1.177547 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
1.955117 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
1.955259 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
1.987992 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
1.988084 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
1.988101 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
2.165320 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
2.165346 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
2.165352 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
2.175081 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
2.175098 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
2.175105 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
2.956439 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
2.956583 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
2.973142 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
2.973237 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
2.973255 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
3.163683 internal in 192.168.1.114 -> 74.125.226.1: icmp: echo request
3.163709 wan2 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
3.163714 eth0 out 172.20.120.130 -> 74.125.226.1: icmp: echo request
3.174329 wan2 in 74.125.226.1 -> 172.20.120.130: icmp: echo reply
3.174362 internal out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
3.174369 eth1 out 74.125.226.1 -> 192.168.1.114: icmp: echo reply
3.957570 internal in 192.168.1.200 -> 4.2.2.2: icmp: echo request
3.957711 wan1 out 172.20.120.123 -> 4.2.2.2: icmp: echo request
3.979899 wan1 in 4.2.2.2 -> 172.20.120.123: icmp: echo reply
3.979990 internal out 4.2.2.2 -> 192.168.1.200: icmp: echo reply
3.980012 eth1 out 4.2.2.2 -> 192.168.1.200: icmp: echo reply

38 packets received by filter
0 packets dropped by kernel

FGT-B #
```

To re-establish the cluster after a failover you need to restart both FortiGate-100D units. Just re-starting FGT-A may not bring the cluster back online.

Chapter 14 - IPsec VPN

This FortiOS Handbook chapter contains the following sections:

IPsec VPN concepts explains the basic concepts that you need to understand about virtual private networks (VPNs).

IPsec VPN overview provides a brief overview of IPsec technology and includes general information about how to configure IPsec VPNs using this guide.

IPsec VPN in the web-based manager describes the IPsec VPN menu of the web-based manager interface.

Gateway-to-gateway configurations explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN. In a gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.

Hub-and-spoke configurations describes how to set up hub-and-spoke IPsec VPNs. In a hub-and-spoke configuration, connections to a number of remote peers and/or clients radiate from a single, central FortiGate hub.

Dynamic DNS configuration describes how to configure a site-to-site VPN, in which one FortiGate unit has a static IP address and the other FortiGate unit has a dynamic IP address and a domain name.

FortiClient dialup-client configurations guides you through configuring a FortiClient dialup-client IPsec VPN. In a FortiClient dialup-client configuration, the FortiGate unit acts as a dialup server and VPN client functionality is provided by the FortiClient Endpoint Security application installed on a remote host.

FortiGate dialup-client configurations explains how to set up a FortiGate dialup-client IPsec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit with a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

Supporting IKE Mode config clients explains how to set up a FortiGate unit as either an IKE Mode Config server or client. IKE Mode Config is an alternative to DHCP over IPsec.

Internet-browsing configuration explains how to support secure web browsing performed by dialup VPN clients, and hosts behind a remote VPN peer. Remote users can access the private network behind the local FortiGate unit and browse the Internet securely. All traffic generated remotely is subject to the security policy that controls traffic on the private network behind the local FortiGate unit.

Redundant VPN configurations discusses the options for supporting redundant and partially redundant tunnels in an IPsec VPN configuration. A FortiGate unit can be configured to support redundant tunnels to the same remote peer if the FortiGate unit has more than one interface to the Internet.

Transparent mode VPNs describes two FortiGate units that create a VPN tunnel between two separate private networks transparently. In transparent mode, all FortiGate unit interfaces except the management interface are invisible at the network layer.

IPv6 IPsec VPNs describes FortiGate unit VPN capabilities for networks based on IPv6 addressing. This includes IPv4-over-IPv6 and IPv6-over-IPv4 tunnelling configurations. IPv6 IPsec VPNs are available in FortiOS 3.0 MR5 and later.

L2TP and IPsec (Microsoft VPN) explains how to support Microsoft Windows native VPN clients.

GRE over IPsec (Cisco VPN) explains how to interoperate with Cisco VPNs that use Generic Routing Encapsulation (GRE) protocol with IPsec.

Protecting OSPF with IPsec provides an example of protecting OSPF links with IPsec.

Redundant OSPF routing over IPsec provides an example of redundant secure communication between two remote networks using an OSPF VPN connection.

OSPF over dynamic IPsec provides an example of how to create a dynamic IPsec VPN tunnel that allows OSPF.

BGP over dynamic IPsec provides an example of how to create a dynamic IPsec VPN tunnel that allows BGP.

Phase 1 parameters provides detailed step-by-step procedures for configuring a FortiGate unit to accept a connection from a remote peer or dialup client. The basic Phase 1 parameters identify the remote peer or clients and support authentication through preshared keys or digital certificates. You can increase VPN connection security further using methods such as extended authentication (XAuth).

Phase 2 parameters provides detailed step-by-step procedures for configuring an IPsec VPN tunnel. During Phase 2, the specific IPsec security associations needed to implement security services are selected and a tunnel is established.

Defining VPN security policies explains how to specify the source and destination IP addresses of traffic transmitted through an IPsec VPN tunnel, and how to define a security encryption policy. Security policies control all IP traffic passing between a source address and a destination address.

Logging and monitoring and Troubleshooting provide VPN monitoring and troubleshooting procedures.

IPsec VPN concepts

Virtual Private Network (VPN) technology enables remote users to connect to private computer networks to gain access to their resources in a secure way. For example, an employee traveling or working from home can use a VPN to securely access the office network through the Internet.

Instead of remotely logging on to a private network using an unencrypted and unsecure Internet connection, the use of a VPN ensures that unauthorized parties cannot access the office network and cannot intercept any of the information that is exchanged between the employee and the office. It is also common to use a VPN to connect the private networks of two or more offices.

Fortinet offers VPN capabilities in the FortiGate Unified Threat Management (UTM) appliance and in the FortiClient Endpoint Security suite of applications. A FortiGate unit can be installed on a private network, and FortiClient software can be installed on the user's computer. It is also possible to use a FortiGate unit to connect to the private network instead of using FortiClient software.

This chapter discusses VPN terms and concepts including:

VPN tunnels
VPN gateways
Clients, servers, and peers
Encryption
Authentication
Phase 1 and Phase 2 settings
Security Association
IKE and IPsec packet processing

VPN tunnels

The data path between a user's computer and a private network through a VPN is referred to as a tunnel. Like a physical tunnel, the data path is accessible only at both ends. In the telecommuting scenario, the tunnel runs between the FortiClient application on the user's PC, or a FortiGate unit or other network device and the FortiGate unit on the office private network.

Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access the data.

Encoded data going through a VPN tunnel

You can create a VPN tunnel between:

- A PC equipped with the FortiClient application and a FortiGate unit
- Two FortiGate units
- Third-party VPN software and a FortiGate unit
  For more information on third-party VPN software, refer to the Fortinet Knowledge Base for more information.

Tunnel templates

Several tunnel templates are available in the IPsec VPN Wizard that cover a variety of different types of IPsec VPN. A list of these templates appear on the first page of the Wizard, located at **VPN > IPsec > Wizard**. The tunnel template list follows.

IPsec VPN Wizard tunnel templates

Template type	Description
Dialup - FortiClient (Windows, MacOS, Android)	On-demand tunnel for users using the FortiClient software.
Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec client.
Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client.
Dialup - Cisco Firewall	On-demand tunnel for users using the Cisco IPsec client.
Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.
Custom VPN Tunnel	No Template.

VPN tunnel list

Once you create an IPsec VPN tunnel, it appears in the VPN tunnel list at **VPN > IPsec > Tunnels**. By default, the tunnel list indicates the name of the tunnel, its interface binding, the tunnel template used, and the tunnel status. If you right-click on the table header row, you can include columns for comments, IKE version, mode (aggressive vs main), phase 2 proposals, and reference number. The tunnel list page also includes the option to create a new tunnel, as well as the options to edit or delete a highlighted tunnel.

VPN gateways

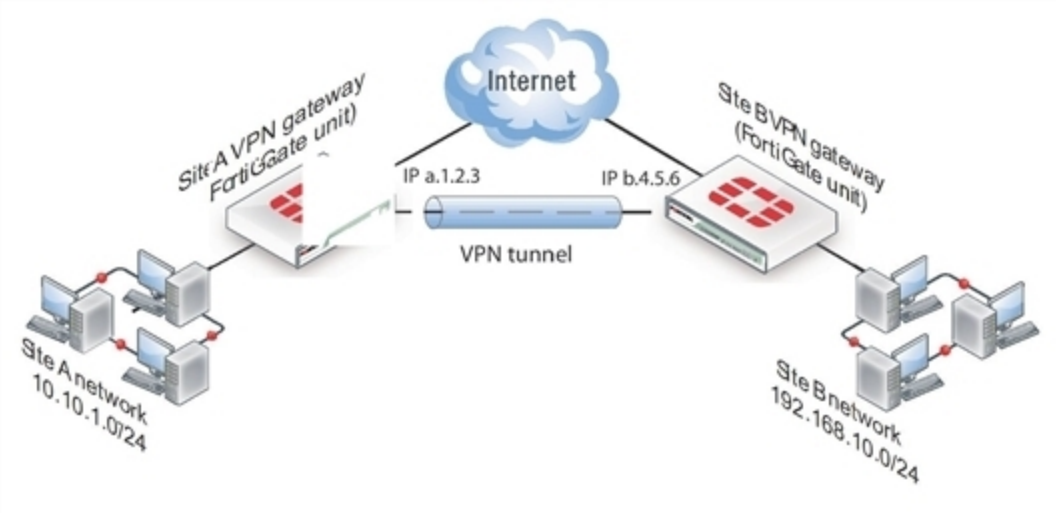
A gateway is a router that connects the local network to other networks. The default gateway setting in your computer's TCP/IP properties specifies the gateway for your local network.

A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets and passes the data packets to the local network. Also, it encrypts data packets destined for the other end of the VPN tunnel, encapsulates them, and sends the IPsec packets to the other VPN gateway. The VPN gateway is a FortiGate unit because the private network behind it is protected, ensuring the security of the unencrypted VPN data. The gateway can also be FortiClient software running on a PC since the unencrypted data is secure on the PC.

The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet. Optionally, you can define a secondary IP address for the interface and use that address as the local VPN gateway address. The benefit of doing this is that your existing setup is not affected by the VPN settings.

The following diagram shows a VPN connection between two private networks with FortiGate units acting as the VPN gateways. This configuration is commonly referred to as Gateway-to-Gateway IPsec VPN.

VPN tunnel between two private networks



Although the IPsec traffic may actually pass through many Internet routers, you can visualize the VPN tunnel as a simple secure connection between the two FortiGate units.

Users on the two private networks do not need to be aware of the VPN tunnel. The applications on their computers generate packets with the appropriate source and destination addresses, as they normally do. The FortiGate units manage all the details of encrypting, encapsulating, and sending the packets to the remote VPN gateway.

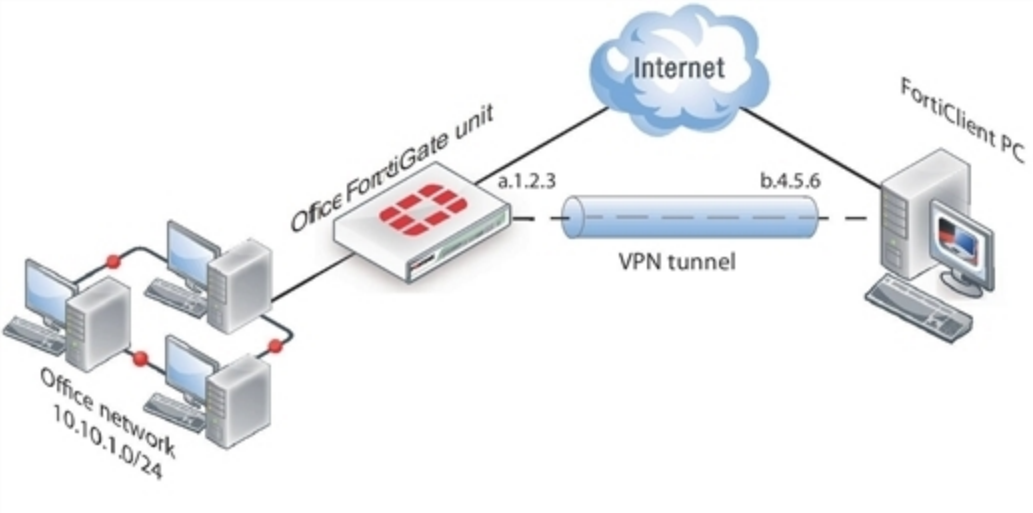
The data is encapsulated in IPsec packets only in the VPN tunnel between the two VPN gateways. Between the user's computer and the gateway, the data is on the secure private network and it is in regular IP packets.

For example User1 on the Site A network, at IP address 10.10.1.7, sends packets with destination IP address 192.168.10.8, the address of User2 on the Site B network. The Site A FortiGate unit is configured to send packets with destinations on the 192.168.10.0 network through the VPN, encrypted and encapsulated. Similarly, the Site B FortiGate unit is configured to send packets with destinations on the 10.10.1.0 network through the VPN tunnel to the Site A VPN gateway.

In the site-to-site, or gateway-to-gateway VPN shown below, the FortiGate units have static (fixed) IP addresses and either unit can initiate communication.

You can also create a VPN tunnel between an individual PC running FortiClient and a FortiGate unit, as shown below. This is commonly referred to as Client-to-Gateway IPsec VPN.

VPN tunnel between a FortiClient PC and a FortiGate unit



On the PC, the FortiClient application acts as the local VPN gateway. Packets destined for the office network are encrypted, encapsulated into IPsec packets, and sent through the VPN tunnel to the FortiGate unit. Packets for other destinations are routed to the Internet as usual. IPsec packets arriving through the tunnel are decrypted to recover the original IP packets.

Clients, servers, and peers

A FortiGate unit in a VPN can have one of the following roles:

- **Server** — responds to a request to establish a VPN tunnel.
- **Client** — contacts a remote VPN gateway and requests a VPN tunnel.
- **Peer** — brings up a VPN tunnel or responds to a request to do so.

The site-to-site VPN shown above is a peer-to-peer relationship. Either FortiGate unit VPN gateway can establish the tunnel and initiate communications. The FortiClient-to-FortiGate VPN shown below is a client-server relationship. The FortiGate unit establishes a tunnel when the FortiClient PC requests one.

A FortiGate unit cannot be a VPN server if it has a dynamically-assigned IP address. VPN clients need to be configured with a static IP address for the server. A FortiGate unit acts as a server only when the remote VPN gateway has a dynamic IP address or is a client-only device or application, such as FortiClient.

As a VPN server, a FortiGate unit can also offer automatic configuration for FortiClient PCs. The user needs to know only the IP address of the FortiGate VPN server and a valid user name/password. FortiClient downloads the VPN configuration settings from the FortiGate VPN server. For information about configuring a FortiGate unit as a VPN server, see the FortiClient Administration Guide.

Encryption

Encryption mathematically transforms data to appear as meaningless random numbers. The original data is called plaintext and the encrypted data is called ciphertext. The opposite process, called decryption, performs the inverse operation to recover the original plaintext from the ciphertext.

The process by which the plaintext is transformed to ciphertext and back again is called an algorithm. All algorithms use a small piece of information, a key, in the arithmetic process of converted plaintext to ciphertext,

or vice-versa. IPsec uses symmetrical algorithms, in which the same key is used to both encrypt and decrypt the data. The security of an encryption algorithm is determined by the length of the key that it uses. FortiGate IPsec VPNs offer the following encryption algorithms, in descending order of security:

AES256	A 128-bit block algorithm that uses a 256-bit key.
AES192	A 128-bit block algorithm that uses a 192-bit key.
AES128	A 128-bit block algorithm that uses a 128-bit key.
3DES	Triple-DES, in which plain text is DES-encrypted three times by three keys.
DES	Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key

The default encryption algorithms provided on FortiGate units make recovery of encrypted data almost impossible without the proper encryption keys.

There is a human factor in the security of encryption. The key must be kept secret, known only to the sender and receiver of the messages. Also, the key must not be something that unauthorized parties might easily guess, such as the sender's name, birthday or simple sequence such as `123456`.

IPsec overheads

The FortiGate sets an IPsec tunnel Maximum Transmission Unit (MTU) of 1436 for 3DES/SHA1 and an MTU of 1412 for AES128/SHA1, as seen with `diag vpn tunnel list`. This indicates that the FortiGate allocates 64 bytes of overhead for 3DES/SHA1 and 88 bytes for AES128/SHA1, which is the difference if you subtract this MTU from a typical ethernet MTU of 1500 bytes.

During the encryption process, AES/DES operates using a specific size of data which is block size. If data is smaller than that, it will be padded for the operation. MD5/SHA-1 HMAC also operates using a specific block size.

The following table describes the potential maximum overhead for each IPsec encryption:

IPsec Transform Set	IPsec Overhead (Max. bytes)
ESP-AES (256, 192, or 128),ESP-SHA-HMAC, or MD5	73
ESP-AES (256, 192, or 128)	61
ESP-3DES, ESP-DES	45
ESP-(DES or 3DES), ESP-SHA-HMAC, or MD5	57
ESP-Null, ESP-SHA-HMAC, or MD5	45
AH-SHA-HMAC or MD5	44

Authentication

To protect data via encryption, a VPN must ensure that only authorized users can access the private network. You must use either a preshared key on both VPN gateways or RSA X.509 security certificates. The examples in this

guide use only preshared key authentication. Refer to the Fortinet Knowledge Base for articles on RSA X.509 security certificates.

Preshared keys

A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration.

Although it looks like a password, the preshared key, also known as a shared secret, is never sent by either gateway. The preshared key is used in the calculations at each end that generate the encryption keys. As soon as the VPN peers attempt to exchange encrypted data, preshared keys that do not match will cause the process to fail.

Additional authentication

To increase security, you can require additional means of authentication from users, such as:

- An identifier, called a peer ID or a local ID.
- Extended authentication (XAUTH) which imposes an additional user name/password requirement.

A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID of a peer is called a Peer ID.

In FortiOS 5.2, new authentication methods have been implemented for IKE: ECDSA-256, ECDSA-384, and ECDSA-521. However, AES-XCBC is not supported.

Phase 1 and Phase 2 settings

A VPN tunnel is established in two phases: Phase 1 and Phase 2. Several parameters determine how this is done. Except for IP addresses, the settings simply need to match at both VPN gateways. There are defaults that are appropriate for most cases.

FortiClient distinguishes between Phase 1 and Phase 2 only in the VPN Advanced settings and uses different terms. Phase 1 is called the IKE Policy. Phase 2 is called the IPsec Policy.

Phase 1

In Phase 1, the two VPN gateways exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

When you configure your FortiGate unit or FortiClient application, you must specify the following settings for Phase 1:

Remote gateway	The remote VPN gateway's address. FortiGate units also have the option of operating only as a server by selecting the "Dialup User" option.
Preshared key	This must be the same at both ends. It is used to encrypt Phase 1 authentication information.
Local interface	The network interface that connects to the other VPN gateway. This applies on a FortiGate unit only.

All other Phase 1 settings have default values. These settings mainly configure the types of encryption to be used. The default settings on FortiGate units and in the FortiClient application are compatible. The examples in this guide use these defaults.

For more detailed information about Phase 1 settings, see Phase 1 parameters on page 1581.

Phase 2

Similar to the Phase 1 process, the two VPN gateways exchange information about the encryption algorithms that they support for Phase 2. You may choose different encryption for Phase 1 and Phase 2. If both gateways have at least one encryption algorithm in common, a VPN tunnel can be established. Keep in mind that more algorithms each phase does not share with the other gateway, the longer negotiations will take. In extreme cases this may cause timeouts during negotiations.

To configure default Phase 2 settings on a FortiGate unit, you need only select the name of the corresponding Phase 1 configuration. In FortiClient, no action is required to enable default Phase 2 settings.

For more detailed information about Phase 2 settings, see Phase 2 parameters on page 1598.

Security Association

The establishment of a Security Association (SA) is the successful outcome of Phase 1 negotiations. Each peer maintains a database of information about VPN connections. The information in each SA can include cryptographic algorithms and keys, keylife, and the current packet sequence number. This information is kept synchronized as the VPN operates. Each SA has a Security Parameter Index (SPI) that is provided to the remote peer at the time the SA is established. Subsequent IPsec packets from the peer always reference the relevant SPI. It is possible for peers to have multiple VPNs active simultaneously, and correspondingly multiple SPIs.

IKE and IPsec packet processing

Internet Key Exchange (IKE) is the protocol used to set up SAs in IPsec negotiation. As described in Phase 1 parameters on page 1581, you can optionally choose IKEv2 over IKEv1 if you configure a route-based IPsec VPN. IKEv2 simplifies the negotiation process, in that it:

- Provides no choice of Aggressive or Main mode in Phase 1.
- Does not support Peer Options or Local ID.
- Does not allow Extended Authentication (XAUTH).
- Allows you to select only one Diffie-Hellman Group.
- Uses less bandwidth.

The following sections identify how IKE versions 1 and 2 operate and differentiate.

IKEv1

Phase 1

A peer, identifed in the IPsec policy configuration, begins the IKE negotiation process. This IKE Security Association (SA) agreement is known as Phase 1. The Phase 1 parameters identify the remote peer or clients and supports authentication through preshared keys or digital certificates. You can increase access security further using peer identifiers, certificate distinguished names, group names, or the FortiGate extended authentication (XAuth) option for authentication purposes. Basically, Phase 1 authenticates a remote peer and sets up a secure communication channel for establishing Phase 2, which negotiates the IPsec SA.

IKE Phase 1 can occur in either Main mode or Aggressive mode. For more information, see Phase 1 parameters on page 1581.

IKE Phase 1 is successful only when the following are true:

- Each peer negotiates a matching IKE SA policy.
- Each peer is authenticated and their identities protected.
- The Diffie-Hellman exchange is authenticated (the pre-shared secret keys match).

For more information on Phase 1, see Phase 1 parameters on page 1581.

Phase 2

Phase 2 parameters define the algorithms that the FortiGate unit can use to encrypt and transfer data for the remainder of the session in an IPsec SA. The basic Phase 2 settings associate IPsec Phase 2 parameters with a Phase 1 configuration.

In Phase 2, the VPN peer or client and the FortiGate unit exchange keys again to establish a more secure communication channel. The Phase 2 Proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of the SA. The keys are generated automatically using a Diffie-Hellman algorithm.

In Phase 2, Quick mode selectors determine which IP addresses can perform IKE negotiations to establish a tunnel. By only allowing authorized IP addresses access to the VPN tunnel, the network is more secure. For more information, see Phase 2 parameters on page 1598.

IKE Phase 2 is successful only when the following are true:

- The IPsec SA is established and protected by the IKE SA.
- The IPsec SA is configured to renegotiate after set durations (see Phase 2 parameters on page 1598 and Phase 2 parameters on page 1598).
- **Optional:** Replay Detection is enabled. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel. See Phase 2 parameters on page 1598.
- **Optional:** Perfect Forward Secrecy (PFS) is enabled. PFS improves security by forcing a new Diffie-Hellman exchange whenever keylife expires. See Phase 2 parameters on page 1598.

For more information on Phase 2, see Phase 2 parameters on page 1598.

With Phase 2 established, the IPsec tunnel is fully negotiated and traffic between the peers is allowed until the SA terminates (for any number of reasons; time-out, interruption, disconnection, etc).

IKEv2

Phase 1

Unlike Phase 1 of IKEv1, IKEv2 does not provide options for Aggressive or Main mode. Furthermore, Phase 1 of IKEv2 begins immediately with an IKE SA initiation, consisting of only two packets (containing all the information typically contained in four packets for IKEv1), securing the channel such that all following transactions are encrypted (see Phase 1 parameters on page 1581).

The encrypted transactions contain the IKE authentication, since remote peers have yet to be authenticated. This stage of IKE authentication in IKEv2 can loosely be called Phase 1.5.

Phase 1.5

As part of this phase, IKE authentication must occur. IKE authentication consists of the following:

- The authentication payloads and Internet Security Association and Key Management Protocol (ISAKMP) identifier.
- The authentication method (RSA, PSK, ECDSA, or EAP).
- The IPsec SA parameters.

Due to the number of authentication methods potentially used, and SAs established, the overall IKEv2 negotiation can range from 4 packets (no EAP exchange at all) to many more.

At this point, both peers have a security association complete and ready to encrypt traffic.

Phase 2

In IKEv1, Phase 2 uses Quick mode to negotiate an IPsec SA between peers. In IKEv2, since the IPsec SA is already established, Phase 2 is essentially only used to negotiate “child” SAs, or to re-key an IPsec SA. That said, there are only two packets for each exchange of this type, similar to the exchange at the outset of Phase 1.5.

IPsec VPN overview

This section provides a brief overview of IPsec technology and includes general information about how to configure IPsec VPNs using this guide.

The following topics are included in this section:

Types of VPNs
Planning your VPN
General preparation steps
How to use this guide to configure an IPsec VPN

VPN configurations interact with the firewall component of the FortiGate unit. There must be a security policy in place to permit traffic to pass between the private network and the VPN tunnel.

Security policies for VPNs specify:

- The FortiGate interface that provides the physical connection to the remote VPN gateway, usually an interface connected to the Internet
- The FortiGate interface that connects to the private network
- IP addresses associated with data that has to be encrypted and decrypted
- Optionally, a schedule that restricts when the VPN can operate
- Optionally, the services (types of data) that can be sent

When the first packet of data that meets all of the conditions of the security policy arrives at the FortiGate unit, a VPN tunnel may be initiated and the encryption or decryption of data is performed automatically afterward. For more information, see Defining VPN security policies on page 1603.

Where possible, you should create route-based VPNs. Generally, route-based VPNs are more flexible and easier to configure than policy-based VPNs — by default they are treated as interfaces. However, these two VPN types have different requirements that limit where they can be used.

Types of VPNs

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify Phase 1 and Phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the Phase 1 and Phase 2 settings.

Route-based VPNs

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy, the virtual interface is the source. In the other policy, the virtual interface is the destination. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

A route-based VPN is also known as an interface-based VPN.

Each route-based IPsec VPN tunnel requires a virtual IPsec interface. As such, the amount of possible route-based IPsec VPNs is limited by the **system.interface** table size. The **system.interface** table size for most devices is 8192.

For a complete list of table sizes for all devices, refer to the Maximum Values table.

Policy-based VPNs

For a policy-based VPN, one security policy enables communication in both directions. You enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

A policy-based VPN is also known as a tunnel-mode VPN.

Comparing policy-based or route-based VPNs

For both VPN types you create Phase 1 and Phase 2 configurations. Both types are handled in the stateful inspection security layer, assuming there is no IPS or AV. For more information on the three security layers, see the FortiOS Troubleshooting guide.

The main difference is in the security policy.

You create a policy-based VPN by defining an IPSEC security policy between two network interfaces and associating it with the VPN tunnel (Phase 1) configuration.

You create a route-based VPN by creating a virtual IPsec interface. You then define a regular ACCEPT security policy to permit traffic to flow between the virtual IPsec interface and another network interface. And lastly, configure a static route to allow traffic over the VPN.

Where possible, you should create route-based VPNs. Generally, route-based VPNs are more flexible and easier to configure than policy-based VPNs — by default they are treated as interfaces. However, these two VPN types have different requirements that limit where they can be used.

Comparison of policy-based and route-based VPNs

Features	Policy-based	Route-based
Both NAT and transparent modes available	Yes	NAT mode only
L2TP-over-IPsec supported	Yes	No
GRE-over-IPsec supported	No	Yes
security policy requirements	Requires a security policy with IPSEC action that specifies the VPN tunnel	Requires only a simple security policy with ACCEPT action
Number of policies per VPN	One policy controls connections in both directions	A separate policy is required for connections in each direction

Planning your VPN

It is a good idea to plan the VPN configuration ahead of time. This will save time later and help you configure your VPN correctly.

All VPN configurations are comprised of numerous required and optional parameters. Before you begin, you need to determine:

- Where the IP traffic originates and where it needs to be delivered
- Which hosts, servers, or networks to include in the VPN
- Which VPN devices to include in the configuration
- Through which interfaces the VPN devices communicate
- Through which interfaces do private networks access the VPN gateways

Once you have this information, you can select a VPN topology that suits the network environment.

Network topologies

The topology of your network will determine how remote peers and clients connect to the VPN and how VPN traffic is routed.

VPN network topologies and brief descriptions

Topology	Description
Gateway-to-gateway configurations	Standard one-to-one VPN between two FortiGate units. See Gateway-to-gateway configurations on page 1609.
Hub-and-spoke configurations	One central FortiGate unit has multiple VPNs to other remote FortiGate units. See Hub-and-spoke configurations on page 1623.
Dynamic DNS configuration	One end of the VPN tunnel has a changing IP address and the other end must go to a dynamic DNS server for the current IP address before establishing a tunnel. See Dynamic DNS configuration on page 1639.
FortiClient dialup-client configurations	Typically remote FortiClient dialup-clients use dynamic IP addresses through NAT devices. The FortiGate unit acts as a dialup server allowing dialup VPN connections from multiple sources. See FortiClient dialup-client configurations on page 1654.
FortiGate dialup-client configurations	Similar to FortiClient dialup-client configurations but with more gateway-to-gateway settings such as unique user authentication for multiple users on a single VPN tunnel. See FortiGate dialup-client configurations on page 1669.
Internet-browsing configuration	Secure web browsing performed by dialup VPN clients, and/or hosts behind a remote VPN peer. See Internet-browsing configuration on page 1682.
Redundant VPN configurations	Options for supporting redundant and partially redundant IPsec VPNs, using route-based approaches. See Redundant VPN configurations on page 1686.
Transparent mode VPNs	In transparent mode, the FortiGate acts as a bridge with all incoming traffic being broadcast back out on all other interfaces. Routing and NAT must be performed on external routers. See Transparent mode VPNs on page 1711.
L2TP and IPsec (Microsoft VPN)	Configure VPN for Microsoft Windows dialup clients using the built in L2TP software. Users do not have to install any See L2TP and IPsec (Microsoft VPN) on page 1730.

These sections contain high-level configuration guidelines with cross-references to detailed configuration procedures. If you need more detail to complete a step, select the cross-reference in the step to drill-down to more detail. Return to the original procedure to complete the procedure. For a general overview of how to configure a VPN, see Planning your VPN .

General preparation steps

A VPN configuration defines relationships between the VPN devices and the private hosts, servers, or networks making up the VPN. Configuring a VPN involves gathering and recording the following information. You will need this information to configure the VPN.

- **The private IP addresses of participating hosts, servers, and/or networks.** These IP addresses represent the source addresses of traffic that is permitted to pass through the VPN. A IP source address can be an individual IP address, an address range, or a subnet address.
- **The public IP addresses of the VPN end-point interfaces.** The VPN devices establish tunnels with each other through these interfaces.
- **The private IP addresses associated with the VPN-device interfaces to the private networks.** Computers on the private networks behind the VPN gateways will connect to their VPN gateways through these interfaces.

How to use this guide to configure an IPsec VPN

This guide uses a task-based approach to provide all of the procedures needed to create different types of VPN configurations. Follow the step-by-step configuration procedures in this guide to set up the VPN.

The following configuration procedures are common to all IPsec VPNs:

1. Define the Phase 1 parameters that the FortiGate unit needs to authenticate remote peers or clients and establish a secure a connection. See Phase 1 parameters on page 1581.
2. Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with a remote peer or dialup client. See Phase 2 parameters on page 1598.
3. Specify the source and destination addresses of IP packets that are to be transported through the VPN tunnel. See Defining VPN security policies on page 1603.
4. Create an IPsec security policy to define the scope of permitted services between the IP source and destination addresses. See Defining VPN security policies on page 1603.

These steps assume you configure the FortiGate unit to generate unique IPsec encryption and authentication keys automatically. In situations where a remote VPN peer or client requires a specific IPsec encryption and authentication key, you must configure the FortiGate unit to use manual keys instead of performing Steps 1 and 2.

IPsec VPN in the web-based manager

To configure an IPsec VPN, use the general procedure below. With these steps, your FortiGate unit will automatically generate unique IPsec encryption and authentication keys. If a remote VPN peer or client requires a specific IPsec encryption or authentication key, you must configure your FortiGate unit to use manual keys instead.

1. Define Phase 1 parameters to authenticate remote peers and clients for a secure connection. See IPsec VPN in the web-based manager on page 1568.
2. Define Phase 2 parameters to create a VPN tunnel with a remote peer or dialup client. See IPsec VPN in the web-based manager on page 1568.
3. Create a security policy to permit communication between your private network and the VPN. Policy-based VPNs have an action of IPSEC, where for interface-based VPNs the security policy action is ACCEPT. See Defining VPN security policies on page 1603.

The FortiGate unit implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. Interface mode, supported in NAT mode only, creates a virtual interface for the local end of a VPN tunnel.

This chapter contains the following sections:

Phase 1 configuration
Phase 2 configuration
Concentrator
IPsec Monitor

Phase 1 configuration

To begin defining the Phase 1 configuration, go to **VPN > IPsec > Tunnels** and select **Create New**. Enter a unique descriptive name for the VPN tunnel and follow the instructions in the VPN Creation Wizard.

The Phase 1 configuration mainly defines the ends of the IPsec tunnel. The remote end is the remote gateway with which the FortiGate unit exchanges IPsec packets. The local end is the FortiGate interface that sends and receives IPsec packets.

If you want to control how the IKE negotiation is processed when there is no traffic, as well as the length of time the FortiGate unit waits for negotiations to occur, you can use the `negotiation-timeout` and `auto-negotiate` commands in the CLI.

For more information, refer to Phase 2 parameters on page 1598 and Phase 2 parameters on page 1598.

Name	Type a name for the Phase 1 definition. The maximum name length is 15 characters for an interface mode VPN, 35 characters for a policy-based VPN. If **Remote Gateway** is **Dialup User**, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on. For a tunnel mode VPN, the name normally reflects where the remote connection originates. For a route-based tunnel, the FortiGate unit also uses the name for the virtual IPsec interface that it creates automatically.
Remote Gateway	Select the category of the remote connection: **Static IP Address** — If the remote peer has a static IP address. **Dialup User** — If one or more FortiClient or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate unit. **Dynamic DNS** — If a remote peer that has a domain name and subscribes to a dynamic DNS service will connect to the FortiGate unit.
IP Address	If you selected **Static IP Address**, enter the IP address of the remote peer.
Dynamic DNS	If you selected ***Dynamic DNS***, enter the domain name of the remote peer.
Local Interface	This option is available in NAT mode only. Select the name of the interface through which remote peers or dialup clients connect to the FortiGate unit. By default, the local VPN gateway IP address is the IP address of the interface that you selected.
Mode	**Main mode** — the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. **Aggressive mode** — the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select Aggressive mode if there is more than one dialup phase1 configuration for the interface IP address. When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select Aggressive mode if there is more than one Phase 1 configuration for the interface IP address and these Phase 1 configurations use different proposals.
Authentication Method	Select **Preshared Key** or **RSA Signature**.

Pre-shared Key	If you selected **Pre-shared Key**, enter the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during Phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.
Certificate Name	If you selected **RSA Signature**, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during Phase 1 negotiations. For information about obtaining and loading the required server certificate, see the FortiOS User Authentication guide.
Peer Options	Peer options are available to authenticate VPN peers or clients, depending on the **Remote Gateway** and **Authentication Method** settings.
Any peer ID	Accept the local ID of any remote VPN peer or client. The FortiGate unit does not check identifiers (local IDs). You can set **Mode** to **Aggressive** or **Main**. You can use this option with RSA Signature authentication. But, for highest security, configure a PKI user/group for the peer and set **Peer Options** to **Accept this peer certificate only**.
This peer ID	This option is available when **Aggressive Mode** is enabled. Enter the identifier that is used to authenticate the remote peer. This identifier must match the Local ID that the remote peer's administrator has configured. If the remote peer is a FortiGate unit, the identifier is specified in the **Local ID** field of the Advanced Phase 1 configuration. If the remote peer is a FortiClient user, the identifier is specified in the **Local ID** field, accessed by selecting **Config** in the **Policy** section of the VPN connection's **Advanced Settings**.
Peer ID from dialup group	Authenticate multiple FortiGate or FortiClient dialup clients that use unique identifiers and unique pre-shared keys (or unique pre-shared keys only) through the same VPN tunnel. You must create a dialup user group for authentication purposes. Select the group from the list next to the **Peer ID from dialup group** option. You must set **Mode** to **Aggressive** when the dialup clients use unique identifiers and unique pre-shared keys. If the dialup clients use unique pre-shared keys only, you can set **Mode** to **Main** if there is only one dialup Phase 1 configuration for this interface IP address.

Phase 1 advanced configuration settings

You can use the following advanced parameters to select the encryption and authentication algorithms that the FortiGate unit uses to generate keys for the IKE exchange. You can also use the following advanced parameters

to ensure the smooth operation of Phase 1 negotiations.

These settings are mainly configured in the CLI, although some options are available after the tunnel is created using the VPN Creation Wizard (using the **Convert to Custom Tunnel** option).

IPv6 Version	Select if you want to use IPv6 addresses for the remote gateway and interface IP addresses.
Local Gateway IP	Specify an IP address for the local end of the VPN tunnel. Select one of the following: **Main Interface IP** — The FortiGate unit obtains the IP address of the interface from the network interface settings. **Specify** — Enter a secondary address of the interface selected in the Phase 1 **Local Interface** field. You cannot configure Interface mode in a transparent mode VDOM.
Phase 1 Proposal	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. Select one of the following symmetric-key encryption algorithms: **DES** — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. **3DES** — Triple-DES; plain text is encrypted three times by three keys. **AES128** — A 128-bit block algorithm that uses a 128-bit key. **AES192** — A 128-bit block algorithm that uses a 192-bit key. **AES256** — A 128-bit block algorithm that uses a 256-bit key.
	You can select either of the following message digests to check the authenticity of messages during an encrypted session: **MD5** — Message Digest 5. **SHA1** — Secure Hash Algorithm 1 - a 160-bit message digest. To specify one combination only, set the **Encryption** and **Authentication** options of the second combination to NULL. To specify a third combination, use the **Add** button beside the fields for the second combination.
Diffie-Hellman Group	Select one or more Diffie-Hellman groups from DH groups 1, 2, 5, and 14 through 21. At least one of the **Diffie-Hellman Group** settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
Keylife	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172 800 seconds.

Local ID	If the FortiGate unit will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the FortiGate unit will supply to the VPN server during the Phase 1 exchange. If the FortiGate unit will act as a VPN client, and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the FortiGate unit will use for authentication purposes. If the FortiGate unit is a dialup client and will not be sharing a tunnel with other dialup clients (that is, the tunnel will be dedicated to this Fortinet dialup client), set **Mode** to **Aggressive**. Note that this Local ID value must match the peer ID value given for the remote VPN peer's Peer Options.
XAuth	This option supports the authentication of dialup clients. It is available for IKE v1 only. **Disable** — Select if you do not use XAuth. **Enable as Client** — If the FortiGate unit is a dialup client, enter the user name and password that the FortiGate unit will need to authenticate itself to the remote XAuth server. **Enable as Server** — This is available only if **Remote Gateway** is set to **Dialup User**. Dialup clients authenticate as members of a dialup user group. You must first create a user group for the dialup clients that need access to the network behind the FortiGate unit. You must also configure the FortiGate unit to forward authentication requests to an external RADIUS or LDAP authentication server. Select a **Server Type** setting to determine the type of encryption method to use between the FortiGate unit, the XAuth client and the external authentication server, and then select the user group from the User Group list.
Username	Enter the user name that is used for authentication.
Password	Enter the password that is used for authentication.
NAT Traversal	Select the check box if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Keepalive Frequency	If you enabled **NAT-traversal**, enter a keepalive frequency setting.

Dead Peer Detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes. With **Dead Peer Detection** selected, you can use the `config vpn ipsec phase1` (tunnel mode) or `config vpn ipsec phase1-interface` (interface mode) CLI command to optionally specify a retry count and a retry interval.

IKE fragmentation

UDP fragmentation can cause issues in IPsec when either the ISP or perimeter firewall(s) cannot pass or fragment the oversized UDP packets that occur when using a very large public security key (PSK). The result is that IPsec tunnels do not come up. The solution is IKE fragmentation.

For most configurations, enabling IKE fragmentation allows connections to automatically establish when they otherwise might have failed due to intermediate nodes dropping IKE messages containing large certificates, which typically push the packet size over 1500 bytes.

FortiOS will fragment a packet on sending if, and only if, all the following are true:

- Phase 1 contains "`set fragmentation enable`".
- The packet is larger than the minimum MTU (576 for IPv4, 1280 for IPv6).
- The packet is being re-transmitted.

By default, IKE fragmentation is enabled, but upon upgrading, any existing phase1-interface may have have "`set fragmentation disable`" added in order to preserve the existing behaviour of not supporting fragmentation.

To enable or disable IKE fragmentation - CLI

```
config vpn ipsec phase1-interface
   edit 1
      set fragmentation [enable | disable]
   next
end
```

Phase 2 configuration

After IPsec Phase 1 negotiations end successfully, you begin Phase 2. You can configure the Phase 2 parameters to define the algorithms that the FortiGate unit may use to encrypt and transfer data for the remainder of the session. During Phase 2, you select specific IPsec security associations needed to implement security services and establish a tunnel.

The basic Phase 2 settings associate IPsec Phase 2 parameters with the Phase 1 configuration that specifies the remote end point of the VPN tunnel. In most cases, you need to configure only basic Phase 2 settings.

These settings are mainly configured in the CLI, although some options are available after the tunnel is created using the VPN Creation Wizard (using the **Convert to Custom Tunnel** option).

Name	Type a name to identify the Phase 2 configuration.
Phase 1	Select the Phase 1 tunnel configuration. For more information on configuring Phase 1, see Phase 1 configuration on page 1568. The Phase 1 configuration describes how remote VPN peers or clients will be authenticated on this tunnel, and how the connection to the remote peer or client will be secured.
Advanced	Define advanced Phase 2 parameters. For more information, see Phase 2 advanced configuration settings below.

Phase 2 advanced configuration settings

In Phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. You select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). These are called Phase 2 Proposal parameters. The keys are generated automatically using a Diffie-Hellman algorithm.

You can use a number of additional advanced Phase 2 settings to enhance the operation of the tunnel.

Phase 2 Proposal	Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to three proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer. Initially there are two proposals. **Add** and **Delete** icons are next to the second **Authentication** field. It is invalid to set both **Encryption** and **Authentication** to **NULL**.
Encryption	Select a symmetric-key algorithms: **NULL** — Do not use an encryption algorithm. **DES** — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. **3DES** — Triple-DES; plain text is encrypted three times by three keys. **AES128** — A 128-bit block algorithm that uses a 128-bit key. **AES192** — A 128-bit block algorithm that uses a 192-bit key. **AES256** — A 128-bit block algorithm that uses a 256-bit key.
Authentication	You can select either of the following message digests to check the authenticity of messages during an encrypted session: **NULL** — Do not use a message digest. **MD5** — Message Digest 5. **SHA1** — Secure Hash Algorithm 1 - a 160-bit message digest. To specify one combination only, set the **Encryption** and **Authentication** options of the second combination to NULL. To specify a third combination, use the ***Add*** button beside the fields for the second combination.
Enable replay detection	Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Enable perfect forward secrecy (PFS)	Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Diffie-Hellman Group	Select one Diffie-Hellman group (1, 2, 5, or 14 through 21). This must match the DH Group that the remote peer or dialup client uses.
Keylife	Select the method for determining when the Phase 2 key expires: **Seconds**, **KBytes**, or **Both**. If you select **Both**, the key expires when either the time has passed or the number of KB have been processed.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.

DHCP-IPsec	Provide IP addresses dynamically to VPN clients. This is available for Phase 2 configurations associated with a dialup Phase 1 configuration. You also need configure a DHCP server or relay on the private network interface. You must configure the DHCP parameters separately. If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the Phase 1 **Peer Options** to **Peer ID from dialup group** and select the appropriate user group. See Phase 1 configuration on page 1568. If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, selecting the check box will cause the FortiGate unit to act as a proxy for the dialup clients.
Quick Mode Selector	Specify the source and destination IP addresses to be used as selectors for IKE negotiations. If the FortiGate unit is a dialup server, keep the default value of 0.0.0.0/0 unless you need to circumvent problems caused by ambiguous IP addresses between one or more of the private networks making up the VPN. You can specify a single host IP address, an IP address range, or a network address. You may optionally specify source and destination port numbers and a protocol number. If you are editing an existing Phase 2 configuration, the **Source address** and **Destination address** fields are unavailable if the tunnel has been configured to use firewall addresses as selectors. This option exists only in the CLI.
Source address	If the FortiGate unit is a dialup server, enter the source IP address that corresponds to the local senders or network behind the local VPN peer (for example, `172.16.5.0/24` or `172.16.5.0/255.255.255.0` for a subnet, or `172.16.5.1/32` or `172.16.5.1/255.255.255.255` for a server or host, or `192.168.10.[80-100]` or `192.168.10.80-192.168.10.100` for an address range). A value of `0.0.0.0/0` means all IP addresses behind the local VPN peer. If the FortiGate unit is a dialup client, source address must refer to the private network behind the Fortinet dialup client.
Source port	Enter the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, type `0`.
Destination address	Enter the destination IP address that corresponds to the recipients or network behind the remote VPN peer (for example, `192.168.20.0/24` for a subnet, or `172.16.5.1/32` for a server or host, or `192.168.10.[80-100]` for an address range). A value of `0.0.0.0/0` means all IP addresses behind the remote VPN peer.

Destination port	Enter the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). To specify all ports, enter `0`.
Protocol	Enter the IP protocol number of the service. To specify all services, enter `0`.

FortiClient VPN

Use the **Dialup - FortiClient (Windows, MacOS, Android)** VPN Wizard option when configuring an IPsec VPN for remote users to connect to the VPN tunnel using FortiClient.

When configuring a FortiClient VPN connection, the settings for Phase 1 and Phase 2 settings are automatically configured by the FortiGate unit. They are set to:

- Remote Gateway — Dialup User
- Mode — Aggressive
- Default settings for Phase 1 and 2 Proposals
- XAUTH Enable as Server (Auto)
- IKE mode-config will be enabled
- Peer Option — “Any peer ID”

The remainder of the settings use the current FortiGate defaults. Note that FortiClient settings need to match these FortiGate defaults. If you need to configure advanced settings for the FortiClient VPN, you must do so using the CLI.

Name	Enter a name for the FortiClient VPN.
Local Outgoing Interface	Select the local outgoing interface for the VPN.
Authentication Method	Select the type of authentication used when logging in to the VPN.
Preshared Key	If **Pre-shared Key** was selected in **Authentication Method**, enter the pre-shared key in the field provided.
User Group	Select a user group. You can also create a user group from the drop-down list by selecting **Create New**.
Address Range Start IP	Enter the start IP address for the DHCP address range for the client.
Address Range End IP	Enter the end IP address for the address range.
Subnet Mask	Enter the subnet mask.
Enable IPv4 Split Tunnel	Enabled by default, this option enables the FortiClient user to use the VPN to access internal resources while other Internet access is not sent over the VPN, alleviating potential traffic bottlenecks in the VPN connection. Disable this option to have all traffic sent through the VPN tunnel.
Accessible Networks	Select from a list of internal networks that the FortiClient user can access.
Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. **Save Password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. **Auto Connect** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. **Always Up (Keep Alive)** - When enabled, if the user selects this option, the FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Endpoint Registration	When selected, the FortiGate unit requests a registration key from FortiClient before a connection can be established. A registration key is defined by going to **System > Config > Advanced**. For more information on FortiClient VPN connections to a FortiGate unit, see the **FortiClient Administration Guide**.

DNS Server	Select which DNS server to use for this VPN: **Use System DNS** — Use the same DNS servers as the FortiGate unit. These are configured at **System > Interface > DNS**. This is the default option. **Specify** — Specify the IP address of a different DNS server.

Concentrator

In a hub-and-spoke configuration, policy-based VPN connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, you can establish VPN tunnels between any two of the remote peers through the FortiGate unit's "hub".

In a hub-and-spoke network, all VPN tunnels terminate at the hub. The peers that connect to the hub are known as "spokes". The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.

You define a concentrator to include spokes in the hub-and-spoke configuration. You create the concentrator in **VPN > IPsec > Concentrator** and select **Create New**. A concentrator configuration specifies which spokes to include in an IPsec hub-and-spoke configuration.

Concentrator Name	Type a name for the concentrator.
Available Tunnels	A list of defined IPsec VPN tunnels. Select a tunnel from the list and then select the right arrow.
Members	A list of tunnels that are members of the concentrator. To remove a tunnel from the concentrator, select the tunnel and select the left arrow.

IPsec Monitor

You can use the IPsec Monitor to view activity on IPsec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels, including tunnel mode and route-based (interface mode) tunnels.

To view the IPsec monitor, go to **VPN > Monitor > IPsec Monitor**.

For dialup VPNs, the list provides status information about the VPN tunnels established by dialup clients, and their IP addresses.

For static IP or dynamic DNS VPNs, the list provides status and IP addressing information about VPN tunnels, active or not, to remote peers that have static IP addresses or domain names. You can also start and stop individual tunnels from the list.

Phase 1 parameters

This chapter provides detailed step-by-step procedures for configuring a FortiGate unit to accept a connection from a remote peer or dialup client. The Phase 1 parameters identify the remote peer or clients and supports authentication through preshared keys or digital certificates. You can increase access security further using peer identifiers, certificate distinguished names, group names, or the FortiGate extended authentication (XAuth) option for authentication purposes.

For more information on Phase 1 parameters in the web-based manager, see IPsec VPN in the web-based manager on page 1568.

The information and procedures in this section do not apply to VPN peers that perform negotiations using manual keys.

The following topics are included in this section:

Overview
Defining the tunnel ends
Choosing Main mode or Aggressive mode
Choosing the IKE version
Authenticating the FortiGate unit
Authenticating remote peers and clients
Defining IKE negotiation parameters
Using XAuth authentication
Dynamic IPsec route control

Overview

To configure IPsec Phase 1 settings, go to **VPN > IPsec > Tunnels** and edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).

IPsec Phase 1 settings define:

- The remote and local ends of the IPsec tunnel
- If Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information (main mode) or in a single message with authentication information that is not encrypted (aggressive mode)
- If a preshared key or digital certificates will be used to authenticate the FortiGate unit to the VPN peer or dialup client
- If the VPN peer or dialup client is required to authenticate to the FortiGate unit. A remote peer or dialup client can authenticate by peer ID or, if the FortiGate unit authenticates by certificate, it can authenticate by peer certificate.
- The IKE negotiation proposals for encryption and authentication
- Optional XAuth authentication, which requires the remote user to enter a user name and password. A FortiGate VPN server can act as an XAuth server to authenticate dialup users. A FortiGate unit that is a dialup client can also be configured as an XAuth client to authenticate itself to the VPN server.

For all the Phase 1 web-based manager fields, see IPsec VPN in the web-based manager on page 1568.

If you want to control how IKE is negotiated when there is no traffic, as well as the length of time the unit waits for negotiations to occur, use the `negotiation-timeout` and `auto-negotiate` commands in the CLI.

Defining the tunnel ends

To begin defining the Phase 1 configuration, go to **VPN > IPsec > Tunnels** and select **Create New**. Enter a unique descriptive name for the VPN tunnel and follow the instructions in the VPN Creation Wizard.

The Phase 1 configuration mainly defines the ends of the IPsec tunnel. The remote end is the remote gateway with which the FortiGate unit exchanges IPsec packets. The local end is the FortiGate interface that sends and receives IPsec packets.

The remote gateway can be:

- A static IP address
- A domain name with a dynamic IP address
- A dialup client

A statically addressed remote gateway is the simplest to configure. You specify the IP address. Unless restricted in the security policy, either the remote peer or a peer on the network behind the FortiGate unit can bring up the tunnel.

If the remote peer has a domain name and subscribes to a dynamic DNS service, you need to specify only the domain name. The FortiGate unit performs a DNS query to determine the appropriate IP address. Unless restricted in the security policy, either the remote peer or a peer on the network behind the FortiGate unit can bring up the tunnel.

If the remote peer is a dialup client, only the dialup client can bring up the tunnel. The IP address of the client is not known until it connects to the FortiGate unit. This configuration is a typical way to provide a VPN for client PCs running VPN client software such as the FortiClient Endpoint Security application.

The local end of the VPN tunnel, the Local Interface, is the FortiGate interface that sends and receives the IPsec packets. This is usually the public interface of the FortiGate unit that is connected to the Internet (typically the WAN1 port). Packets from this interface pass to the private network through a security policy.

By default, the local VPN gateway is the IP address of the selected Local Interface. If you are configuring an interface mode VPN, you can optionally use a secondary IP address of the Local Interface as the local gateway.

Choosing Main mode or Aggressive mode

The FortiGate unit and the remote peer or dialup client exchange Phase 1 parameters in either Main mode or Aggressive mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.

- In **Main** mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information
- In **Aggressive** mode, the Phase 1 parameters are exchanged in a single message with unencrypted authentication information.

Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID. Aggressive mode might not be as secure as Main mode, but the advantage to Aggressive mode is that it is faster than Main mode (since fewer packets are exchanged). Aggressive mode is typically used for remote access VPN's. But you would also use aggressive mode if one or both peers have dynamic external IP addresses. Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.

Choosing the IKE version

If you create a route-based VPN, you have the option of selecting IKE version 2. Otherwise, IKE version 1 is used.

IKEv2, defined in RFC 4306, simplifies the negotiation process that creates the security association (SA).

If you select IKEv2:

- There is no choice in Phase 1 of Aggressive or Main mode.
- FortiOS does not support Peer Options or Local ID.
- Extended Authentication (XAUTH) is not available.
- You can select only one Diffie-Hellman Group.
- You can utilize EAP and MOBIKE.

IKEv2 cookie notification for IKE_SA_INIT

IKEv2 offers an optional exchange within IKE_SA_INIT (the initial exchange between peers when establishing a secure tunnel) as a reuslt of an inherent vulnerability in IPsec implementations, as described in RFC 5996.

Two expected attacks against IKE are state and CPU exhaustion, where the target is flooded with session initiation requests from forged IP addresses. These attacks can be made less effective if a responder uses minimal CPU and commits no state to an SA until it knows the initiator can receive packets at the address from which it claims to be sending them.

If the IKE_SA_INIT response includes the cookie notification, the initiator MUST then retry the IKE_SA_INIT request, and include the cookie notification containing the received data as the first payload, and all other payloads unchanged.

Upon detecting that the number of half-open IKEv2 SAs is above the threshold value, the VPN dialup server requires all future SA_INIT requests to include a valid cookie notification payload that the server sends back, in order to preserve CPU and memory resources.

For most devices, the threshold value is set to 500, half of the maximum 1,000 connections.

This feature is enabled by default in FortiOS 5.2.

Authenticating the FortiGate unit

The FortiGate unit can authenticate itself to remote peers or dialup clients using either a pre-shared key or an RSA Signature (certificate).

Authenticating the FortiGate unit with digital certificates

To authenticate the FortiGate unit using digital certificates, you must have the required certificates installed on the remote peer and on the FortiGate unit. The signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer. If you use certificates to authenticate the FortiGate unit, you can also require the remote peers or dialup clients to authenticate using certificates.

For more information about obtaining and installing certificates, see the FortiOS User Authentication guide.

To authenticate the FortiGate unit using digital certificates

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button):

Name	Enter a name that reflects the origination of the remote connection. For interface mode, the name can be up to 15 characters long.
Remote Gateway	Select the nature of the remote connection. Each option changes the available fields you must configure. For more information, see Authenticating the FortiGate unit on page 1583.
Local Interface	Select the interface that is the local end of the IPsec tunnel. For more information, see Authenticating the FortiGate unit on page 1583. The local interface is typically the WAN1 port.
Mode	Select a mode. It is easier to use Aggressive mode. In **Main** mode, parameters are exchanged in multiple encrypted rounds. In **Aggressive** mode, parameters are exchanged in a single unencrypted message. Aggressive mode must be used when the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID). For more information, see Authenticating the FortiGate unit on page 1583.
Authentication Method	Select **Signature.**
Certificate Name	Select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during Phase 1 negotiations. You must obtain and load the required server certificate before this selection. See the FortiOS User Authentication guide. If you have not loaded any certificates, use the certificate named **Fortinet_Factory**.
Peer Options	Peer options define the authentication requirements for remote peers or dialup clients. They are not for your FortiGate unit itself. See Authenticating the FortiGate unit on page 1583.
Advanced	You can use the default settings for most Phase 1 configurations. Changes are required only if your network requires them. These settings includes IKE version, DNS server, P1 proposal encryption and authentication settings, and XAuth settings. See Authenticating the FortiGate unit on page 1583.

3. If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters in the Advanced section. See Authenticating the FortiGate unit on page 1583.
4. Select **OK**.

Authenticating the FortiGate unit with a pre-shared key

The simplest way to authenticate a FortiGate unit to its remote peers or dialup clients is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth). Also, you need to have a secure way to distribute the pre-shared key to the peers.

If you use pre-shared key authentication alone, all remote peers and dialup clients must be configured with the same pre-shared key. Optionally, you can configure remote peers and dialup clients with unique pre-shared keys. On the FortiGate unit, these are configured in user accounts, not in the phase_1 settings. For more information, see Authenticating the FortiGate unit on page 1583.

The pre-shared key must contain at least 6 printable characters and best practices dictate that it be known only to network administrators. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.

If you authenticate the FortiGate unit using a pre-shared key, you can require remote peers or dialup clients to authenticate using peer IDs, but not client certificates.

To authenticate the FortiGate unit with a pre-shared key

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button):

Name	Enter a name that reflects the origination of the remote connection.
Remote Gateway	Select the nature of the remote connection. For more information, see Authenticating the FortiGate unit on page 1583.
Local Interface	Select the interface that is the local end of the IPsec tunnel. For more information, see Authenticating the FortiGate unit on page 1583. The local interface is typically the WAN1 port.
Mode	Select Main or Aggressive mode. In **Main** mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. In **Aggressive** mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. When the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID), you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address. For more information, see Authenticating the FortiGate unit on page 1583.
Authentication Method	Select **Pre-shared Key**.

Pre-shared Key	Enter the preshared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during Phase 1 negotiations. You must define the same value at the remote peer or client. The key must contain at least 6 printable characters and best practices dictate that it only be known by network administrators. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.
Peer options	Peer options define the authentication requirements for remote peers or dialup clients, not for the FortiGate unit itself. You can require the use of peer IDs, but not client certificates. For more information, see Authenticating the FortiGate unit on page 1583.
Advanced	You can retain the default settings unless changes are needed to meet your specific requirements. See Authenticating the FortiGate unit on page 1583.

3. If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters. See Authenticating the FortiGate unit on page 1583.
4. Select **OK**.

Authenticating remote peers and clients

Certificates or pre-shared keys restrict who can access the VPN tunnel, but they do not identify or authenticate the remote peers or dialup clients. You have the following options for authentication:

Methods of authenticating remote VPN peers

Certificates or Pre-shared key	Local ID	User account pre-shared keys	Reference
Certificates			See Enabling VPN access for specific certificate holders on page 1587.
Either	**X**		See Enabling VPN access by peer identifier on page 1588.
Pre-shared key		**X**	See Enabling VPN access with user accounts and pre-shared keys on page 1589.
Pre-shared key	**X**	**X**	See Enabling VPN access with user accounts and pre-shared keys on page 1589.

For authentication of users of the remote peer or dialup client device, see Authenticating remote peers and clients on page 1586.

Enabling VPN access for specific certificate holders

When a VPN peer or dialup client is configured to authenticate using digital certificates, it sends the Distinguished Name (DN) of its certificate to the FortiGate unit. This DN can be used to allow VPN access for the certificate holder. That is, a FortiGate unit can be configured to deny connections to all remote peers and dialup clients except the one having the specified DN.

Before you begin

The following procedures assume that you already have an existing Phase 1 configuration (see Authenticating remote peers and clients on page 1586). Follow the procedures below to add certificate-based authentication parameters to the existing configuration.

Before you begin, you must obtain the certificate DN of the remote peer or dialup client. If you are using the FortiClient application as a dialup client, refer to FortiClient online help for information about how to view the certificate DN. To view the certificate DN of a FortiGate unit, see To view server certificate information and obtain the local DN on page 1587.

Use the `config user peer` CLI command to load the DN value into the FortiGate configuration. For example, if a remote VPN peer uses server certificates issued by your own organization, you would enter information similar to the following:

```
config user peer
   edit DN_FG1000
      set cn 192.168.2.160
      set cn-type ipv4
end
```

The value that you specify to identify the entry (for example, DN_FG1000) is displayed in the **Accept this peer certificate only** list in the IPsec Phase 1 configuration when you return to the web-based manager.

If the remote VPN peer has a CA-issued certificate to support a higher level of credibility, you would enter information similar to the following in the CLI:

```
config user peer
   edit CA_FG1000
      set ca CA_Cert_1
      set subject FG1000_at_site1
end
```

The value that you specify to identify the entry (for example, CA_FG1000) is displayed in the Accept this peer certificate only list in the IPsec Phase 1 configuration when you return to the web-based manager. For more information about these CLI commands, see the “user” chapter of the FortiGate CLI Reference.

A group of certificate holders can be created based on existing user accounts for dialup clients. To create the user accounts for dialup clients, see the “User” chapter of the FortiGate Administration Guide. To create the certificate group afterward, use the `config user peergrp` CLI command. See the “user” chapter of the FortiGate CLI Reference.

To view server certificate information and obtain the local DN

1. Go to **System > Certificates > Local Certificates**.
2. Note the CN value in the **Subject** field (for example, `CN = 172.16.10.125`, `CN = info@fortinet.com`, or `CN = www.example.com`).

To view CA root certificate information and obtain the CA certificate name

1. Go to **System > Certificates > CA Certificates**.
2. Note the value in the **Name** column (for example, `CA_Cert_1`).

Configuring certificate authentication for a VPN

With peer certificates loaded, peer users and peer groups defined, you can configure your VPN to authenticate users by certificate.

To enable access for a specific certificate holder or a group of certificate holders

1. At the FortiGate VPN server, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. From the **Authentication Method** list, select **RSA Signature**.
4. From the **Certificate Name** list, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client
5. Under **Peer Options**, select one of these options:
   - To accept a specific certificate holder, select **Accept this peer certificate only** and select the name of the certificate that belongs to the remote peer or dialup client. The certificate DN must be added to the FortiGate configuration through CLI commands before it can be selected here. See Before you begin on page 1587.
   - To accept dialup clients who are members of a certificate group, select **Accept this peer certificate group only** and select the name of the group. The group must be added to the FortiGate configuration through CLI commands before it can be selected here. See Before you begin on page 1587.
6. If you want the FortiGate VPN server to supply the DN of a local server certificate for authentication purposes, select **Advanced** and then from the **Local ID** list, select the DN of the certificate that the FortiGate VPN server is to use.
7. Select **OK**.

Enabling VPN access by peer identifier

Whether you use certificates or pre-shared keys to authenticate the FortiGate unit, you can require that remote peers or clients have a particular peer ID. This adds another piece of information that is required to gain access to the VPN. More than one FortiGate/FortiClient dialup client may connect through the same VPN tunnel when the dialup clients share a preshared key and assume the same identifier.

A peer ID, also called local ID, can be up to 63 characters long containing standard regular expression characters. Local ID is set in phase1 Aggressive Mode configuration.

You cannot require a peer ID for a remote peer or client that uses a pre-shared key and has a static IP address.

To authenticate remote peers or dialup clients using one peer ID

1. At the FortiGate VPN server, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Select **Aggressive** mode in any of the following cases:
   - The FortiGate VPN server authenticates a FortiGate dialup client that uses a dedicated tunnel
   - A FortiGate unit has a dynamic IP address and subscribes to a dynamic DNS service

- FortiGate/FortiClient dialup clients sharing the same preshared key and local ID connect through the same VPN tunnel

4. For the **Peer Options**, select **This peer ID** and type the identifier into the corresponding field.
5. Select **OK**.

To assign an identifier (local ID) to a FortiGate unit

Use this procedure to assign a peer ID to a FortiGate unit that acts as a remote peer or dialup client.

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Select **Advanced**.
4. In the **Local ID** field, type the identifier that the FortiGate unit will use to identify itself.
5. Set **Mode** to **Aggressive** if any of the following conditions apply:
   - The FortiGate unit is a dialup client that will use a unique ID to connect to a FortiGate dialup server through a dedicated tunnel.
   - The FortiGate unit has a dynamic IP address, subscribes to a dynamic DNS service, and will use a unique ID to connect to the remote VPN peer through a dedicated tunnel.
   - The FortiGate unit is a dialup client that shares the specified ID with multiple dialup clients to connect to a FortiGate dialup server through the same tunnel.
6. Select **OK**.

To configure the FortiClient application

Follow this procedure to add a peer ID to an existing FortiClient configuration:

1. Start the FortiClient application.
2. Go to **VPN > Connections**, select the existing configuration.
3. Select **Advanced > Edit > Advanced**.
4. Under **Policy**, select **Config**.
5. In the **Local ID** field, type the identifier that will be shared by all dialup clients. This value must match the **This peer ID** value that you specified previously in the Phase 1 gateway configuration on the FortiGate unit.
6. Select **OK** to close all dialog boxes.
7. Configure all dialup clients the same way using the same preshared key and local ID.

Enabling VPN access with user accounts and pre-shared keys

You can permit access only to remote peers or dialup clients that have pre-shared keys and/or peer IDs configured in user accounts on the FortiGate unit.

If you want two VPN peers (or a FortiGate unit and a dialup client) to accept reciprocal connections based on peer IDs, you must enable the exchange of their identifiers when you define the Phase 1 parameters.

The following procedures assume that you already have an existing Phase 1 configuration (see Authenticating remote peers and clients on page 1586). Follow the procedures below to add ID checking to the existing configuration.

Before you begin, you must obtain the identifier (local ID) of the remote peer or dialup client. If you are using the FortiClient Endpoint Security application as a dialup client, refer to the Authenticating FortiClient Dialup Clients Technical Note to view or assign an identifier. To assign an identifier to a FortiGate dialup client or a FortiGate

unit that has a dynamic IP address and subscribes to a dynamic DNS service, see To assign an identifier (local ID) to a FortiGate unit on page 1589.

If required, a dialup user group can be created from existing user accounts for dialup clients. To create the user accounts and user groups, see the User Authentication handbook chapter.

The following procedure supports FortiGate/FortiClient dialup clients that use unique preshared keys and/or peer IDs. The client must have an account on the FortiGate unit and be a member of the dialup user group.

The dialup user group must be added to the FortiGate configuration before it can be selected. For more information, see the User Authentication handbook chapter.

The FortiGate dialup server compares the local ID that you specify at each dialup client to the FortiGate user-account user name. The dialup-client preshared key is compared to a FortiGate user-account password.

To authenticate dialup clients using unique preshared keys and/or peer IDs

1. At the FortiGate VPN server, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. If the clients have unique peer IDs, set **Mode** to **Aggressive**.
4. Clear the **Pre-shared Key** field.
   The user account password will be used as the preshared key.
5. Select **Peer ID from dialup group** and then select the group name from the list of user groups.
6. Select **OK**.

Follow this procedure to add a unique pre-shared key and unique peer ID to an existing FortiClient configuration.

To configure FortiClient - pre-shared key and peer ID

1. Start the FortiClient Endpoint Security application.
2. Go to **VPN > Connections**, select the existing configuration.
3. Select **Advanced > Edit**.
4. In the **Preshared Key** field, type the FortiGate password that belongs to the dialup client (for example, `1234546`).
   The user account password will be used as the preshared key.
5. Select **Advanced**.
6. Under **Policy**, select **Config**.
7. In the **Local ID** field, type the FortiGate user name that you assigned previously to the dialup client (for example, `FortiClient1`).
8. Select **OK** to close all dialog boxes.

Configure all FortiClient dialup clients this way using unique preshared keys and local IDs.

Follow this procedure to add a unique pre-shared key to an existing FortiClient configuration.

To configure FortiClient - preshared key only

1. Start the FortiClient Endpoint Security application.
2. Go to **VPN > Connections**, select the existing configuration
3. Select **Advanced > Edit**.

4. In the **Preshared Key** field, type the user name, followed by a "+" sign, followed by the password that you specified previously in the user account settings on the FortiGate unit (for example, `FC2+1FG6LK`)
5. Select **OK** to close all dialog boxes.

Configure all the FortiClient dialup clients this way using their unique peer ID and pre-shared key values.

Defining IKE negotiation parameters

In Phase 1, the two peers exchange keys to establish a secure communication channel between them. As part of the Phase 1 process, the two peers authenticate each other and negotiate a way to encrypt further communications for the duration of the session. For more information see Defining IKE negotiation parameters on page 1591. The Phase 1 Proposal parameters select the encryption and authentication algorithms that are used to generate keys for protecting negotiations.

The IKE negotiation parameters determine:

- Which encryption algorithms may be applied for converting messages into a form that only the intended recipient can read
- Which authentication hash may be used for creating a keyed hash from a preshared or private key
- Which Diffie-Hellman group (DH Group) will be used to generate a secret session key

Phase 1 negotiations (in main mode or aggressive mode) begin as soon as a remote VPN peer or client attempts to establish a connection with the FortiGate unit. Initially, the remote peer or dialup client sends the FortiGate unit a list of potential cryptographic parameters along with a session ID. The FortiGate unit compares those parameters to its own list of advanced Phase 1 parameters and responds with its choice of matching parameters to use for authenticating and encrypting packets. The two peers handle the exchange of encryption keys between them, and authenticate the exchange through a preshared key or a digital signature.

Generating keys to authenticate an exchange

The FortiGate unit supports the generation of secret session keys automatically using a Diffie-Hellman algorithm. These algorithms are defined in RFC 2409. The **Keylife** setting in the **Phase 1 Proposal** area determines the amount of time before the Phase 1 key expires. Phase 1 negotiations are re-keyed automatically when there is an active security association. See Dead peer detection on page 1594.

You can enable or disable automatic re-keying between IKE peers through the `phase1-rekey` attribute of the `config system global` CLI command. For more information, see the "System" chapter of the FortiGate CLI Reference.

When in FIPS-CC mode, the FortiGate unit requires DH key exchange to use values at least 3072 bits long. However most browsers need the key size set to 1024. You can set the minimum size of the DH keys in the CLI.

```
config system global
     set dh-params 3072
end
```

When you use a preshared key (shared secret) to set up two-party authentication, the remote VPN peer or client and the FortiGate unit must both be configured with the same preshared key. Each party uses a session key derived from the Diffie-Hellman exchange to create an authentication key, which is used to sign a known combination of inputs using an authentication algorithm (such as HMAC-MD5, HMAC-SHA-1, or HMAC-SHA-256). Hash-based Message Authentication Code (HMAC) is a method for calculating an authentication code

using a hash function plus a secret key, and is defined in RFC 2104. Each party signs a different combination of inputs and the other party verifies that the same result can be computed.

For information regarding NP accelerated offloading of IPsec VPN authentication algorithms, please refer to the Hardware Acceleration handbook chapter.

When you use preshared keys to authenticate VPN peers or clients, you must distribute matching information to all VPN peers and/or clients whenever the preshared key changes.

As an alternative, the remote peer or dialup client and FortiGate unit can exchange digital signatures to validate each other's identity with respect to their public keys. In this case, the required digital certificates must be installed on the remote peer and on the FortiGate unit. By exchanging certificate DNs, the signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer.

The following procedure assumes that you already have a Phase 1 definition that describes how remote VPN peers and clients will be authenticated when they attempt to connect to a local FortiGate unit. For information about the Local ID and XAuth options, see Defining IKE negotiation parameters on page 1591 and Defining IKE negotiation parameters on page 1591. Follow this procedure to add IKE negotiation parameters to the existing definition.

Defining IKE negotiation parameters

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Select **Phase 1 Proposal** and include the appropriate entries as follows:

Phase 1 Proposal	Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define. It is invalid to set both **Encryption** and **Authentication** to null.
Encryption	Select a symmetric-key algorithms: **NULL** — Do not use an encryption algorithm. **DES** — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. **3DES** — Triple-DES; plain text is encrypted three times by three keys. **AES128** — A 128-bit block algorithm that uses a 128-bit key. **AES192** — A 128-bit block algorithm that uses a 192-bit key. **AES256** — A 128-bit block algorithm that uses a 256-bit key.

Authentication	You can select either of the following message digests to check the authenticity of messages during an encrypted session: **NULL** — Do not use a message digest. **MD5** — Message Digest 5. **SHA1** — Secure Hash Algorithm 1 - a 160-bit message digest. To specify one combination only, set the **Encryption** and **Authentication** options of the second combination to NULL. To specify a third combination, use the **Add** button beside the fields for the second combination. For information regarding NP accelerated offloading of IPsec VPN authentication algorithms, please refer to the Hardware Acceleration handbook chapter.
Diffie-Hellman Group	Select one or more Diffie-Hellman groups from DH groups 1, 2, 5, and 14 through 21. When using aggressive mode, DH groups cannot be negotiated. By default, DH group 14 is selected, to provide sufficient protection for stronger cipher suites that include AES and SHA2. If you select multiple DH groups, the order they appear in the configuration is the order in which they are negotiates. If both VPN peers (or a VPN server and its client) have static IP addresses and use aggressive mode, select a single DH group. The setting on the FortiGate unit must be identical to the setting on the remote peer or dialup client. When the remote VPN peer or client has a dynamic IP address and uses aggressive mode, select up to three DH groups on the FortiGate unit and one DH group on the remote peer or dialup client. The setting on the remote peer or dialup client must be identical to one of the selections on the FortiGate unit. If the VPN peer or client employs main mode, you can select multiple DH groups. At least one of the settings on the remote peer or dialup client must be identical to the selections on the FortiGate unit.
Keylife	Type the amount of time (in seconds) that will be allowed to pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Nat-traversal	Enable this option if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared). When in doubt, enable NAT-traversal. See NAT traversal on page 1594.
Keepalive Frequency	If you enabled NAT traversal, enter a keepalive frequency setting. The value represents an interval from 0 to 900 seconds where the connection will be maintained with no activity. For additional security this value must be as low as possible. See NAT keepalive frequency on page 1594.

Dead Peer Detection	Enable this option to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. This feature minimizes the traffic required to check if a VPN peer is available or unavailable (dead). See Dead peer detection on page 1594.

NAT traversal

Network Address Translation (NAT) is a way to convert private IP addresses to publicly routable Internet addresses and vise versa. When an IP packet passes through a NAT device, the source or destination address in the IP header is modified. FortiGate units support NAT version 1 (encapsulate on port 500 with non-IKE marker), version 3 (encapsulate on port 4500 with non-ESP marker), and compatible versions.

NAT cannot be performed on IPsec packets in ESP tunnel mode because the packets do not contain a port number. As a result, the packets cannot be demultiplexed. To work around this, the FortiGate unit provides a way to protect IPsec packet headers from NAT modifications. When the Nat-traversal option is enabled, outbound encrypted packets are wrapped inside a UDP IP header that contains a port number. This extra encapsulation allows NAT devices to change the port number without modifying the IPsec packet directly.

To provide the extra layer of encapsulation on IPsec packets, the Nat-traversal option must be enabled whenever a NAT device exists between two FortiGate VPN peers or a FortiGate unit and a dialup client such as FortiClient. On the receiving end, the FortiGate unit or FortiClient removes the extra layer of encapsulation before decrypting the packet.

NAT keepalive frequency

When a NAT device performs network address translation on a flow of packets, the NAT device determines how long the new address will remain valid if the flow of traffic stops (for example, the connected VPN peer may be idle). The device may reclaim and reuse a NAT address when a connection remains idle for too long.

To work around this, when you enable NAT traversal specify how often the FortiGate unit sends periodic keepalive packets through the NAT device in order to ensure that the NAT address mapping does not change during the lifetime of a session. To be effective, the keepalive interval must be smaller than the session lifetime value used by the NAT device.

The keepalive packet is a 138-byte ISAKMP exchange.

Dead peer detection

Sometimes, due to routing issues or other difficulties, the communication link between a FortiGate unit and a VPN peer or client may go down. Packets could be lost if the connection is left to time out on its own. The FortiGate unit provides a mechanism called Dead Peer Detection, sometimes referred to as gateway detection or ping server, to prevent this situation and reestablish IKE negotiations automatically before a connection times out: the active Phase 1 security associations are caught and renegotiated (rekeyed) before the Phase 1 encryption key expires.

By default, Dead Peer Detection sends probe messages every five seconds by default (see `dpd-retryinterval` in the FortiGate CLI Reference). If you are experiencing high network traffic, you can experiment with increasing the ping interval. However longer intervals will require more traffic to detect dead peers which will result in more traffic.

In the web-based manager, the Dead Peer Detection option can be enabled when you define advanced Phase 1 options. The `config vpn ipsec phase1` CLI command supports additional options for specifying a retry count and a retry interval.

For more information about these commands and the related `config router gwdetect` CLI command, see the FortiGate CLI Reference.

For example, enter the following CLI commands to configure dead peer detection on the existing IPsec Phase 1 configuration called `test` to use 15 second intervals and to wait for 3 missed attempts before declaring the peer dead and taking action.

```
config vpn ipsec phase1
   edit test
      set dpd enable
      set dpd-retryinveral 15
      set dpd-retrycount 3
   next
end
```

Using XAuth authentication

Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate in a separate exchange at the end of Phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS, and LDAP to authenticate dialup clients. You can configure a FortiGate unit to function either as an XAuth server or an XAuth client.If the server or client is attempting a connection using XAuth and the other end is not using XAuth, the failed connection attempts that are logged will not specify XAuth as the reason.

Using the FortiGate unit as an XAuth server

A FortiGate unit can act as an XAuth server for dialup clients. When the Phase 1 negotiation completes, the FortiGate unit challenges the user for a user name and password. It then forwards the user's credentials to an external RADIUS or LDAP server for verification.

If the user records on the RADIUS server have suitably configured Framed-IP-Address fields, you can assign client virtual IP addresses by XAuth instead of from a DHCP address range. See FortiClient dialup-client configurations on page 1654.

The authentication protocol to use for XAuth depends on the capabilities of the authentication server and the XAuth client:

- Select **PAP Server** whenever possible.
- You must select **PAP Server** for all implementations of LDAP and some implementations of Microsoft RADIUS.
- Select **Auto Server** when the authentication server supports **CHAP Server** but the XAuth client does not. The FortiGate unit will use PAP to communicate with the XAuth client and CHAP to communicate with the authentication server. You can also use **Auto Server** to allows multiple source interfaces to be defined in an IPsec/IKE policy

Before you begin, create user accounts and user groups to identify the dialup clients that need to access the network behind the FortiGate dialup server. If password protection will be provided through an external RADIUS or LDAP server, you must configure the FortiGate dialup server to forward authentication requests to the authentication server. For information about these topics, see the FortiGate User Authentication Guide.

To authenticate a dialup user group using XAuth settings

1. At the FortiGate dialup server, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the *Convert to Custom Tunnel* button).
3. Under **XAuth**, select the **Server Type** setting, which determines the type of encryption method to use between the XAuth client, the FortiGate unit and the authentication server. Select one of the following options:
   - **PAP Server** —Password Authentication Protocol.
   - **CHAP Server** — Challenge-Handshake Authentication Protocol.
   - **Auto Server** —Use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server. This option allows multiple source interfaces to be defined in an IPsec/IKE policy.
4. From the **User Group** list, select the user group that needs to access the private network behind the FortiGate unit. The group must be added to the FortiGate configuration before it can be selected here. For multiple source interfaces to be defined in the IPsec/IKE policy, select **Inherit Groups from Policy**.
5. Select **OK**.

Using the FortiGate unit as an XAuth client

If the FortiGate unit acts as a dialup client, the remote peer, acting as an XAuth server, might require a username and password. You can configure the FortiGate unit as an XAuth client, with its own username and password, which it provides when challenged.

To configure the FortiGate dialup client as an XAuth client

1. At the FortiGate dialup client, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Under **XAuth**, select **Enable as Client**.
4. In the **Username** field, type the FortiGate PAP, CHAP, RADIUS, or LDAP user name that the FortiGate XAuth server will compare to its records when the FortiGate XAuth client attempts to connect.
5. In the **Password** field, type the password to associate with the user name.
6. Select **OK**.

Dynamic IPsec route control

You can add a route to a peer destination selector by using the `add-route` option, which is available for all dynamic IPsec Phases 1 and 2, for both policy-based and route-based IPsec VPNs. This option was previously only available when `mode-cfg` was enabled in Phase 1.

The add-route option adds a route to the FortiGate unit's routing information base when the dynamic tunnel is negotiated. You can use the distance and priority options to set the distance and priority of this route. If this results in a route with the lowest distance, it is added to the FortiGate unit's forwarding information base.

You can also enable add-route in any policy-based or route-based Phase 2 configuration that is associated with a dynamic (dialup) Phase 1. In Phase 2, add-route can be enabled, disabled, or set to use the same route as Phase 1.

The add-route feature is enabled by default and is configured in the CLI.

Syntax

Phase 1

```
config vpn ipsec
   edit <name>
      set type dynamic
      set add-route {enable | disable}
   end
end
```

Phase 2

```
config vpn ipsec {phase2 | phase2-interface}
   edit <name>
      set add-route {phase1 | enable | disable}
   end
end
```

Blocking IPsec SA Negotiation

For interface-based IPsec, IPsec SA negotiation blocking can only be removed if the peer offers a wildcard selector. If a wildcard selector is offered then the wildcard route will be added to the routing table with the distance/priority value configured in Phase 1 and, if that is the route with the lowest distance, it is installed into the forwarding information base.

In cases where this occurs, it is important to ensure that the distance value configured on Phase 1 is set appropriately.

Phase 2 parameters

This section describes the Phase 2 parameters that are required to establish communication through a VPN.

The following topics are included in this section:

Phase 2 settings
Configuring the Phase 2 parameters

Phase 2 settings

After IPsec VPN Phase 1 negotiations complete successfully, Phase 2 negotiation begins. Phase 2 parameters define the algorithms that the FortiGate unit can use to encrypt and transfer data for the remainder of the session. The basic Phase 2 settings associate IPsec Phase 2 parameters with a Phase 1 configuration.

When defining Phase 2 parameters, you can choose any set of Phase 1 parameters to set up a secure connection and authenticate the remote peer.

For more information on Phase 2 settings in the web-based manager, see IPsec VPN in the web-based manager on page 1568.

The information and procedures in this section do not apply to VPN peers that perform negotiations using manual keys.

Phase 2 Proposals

In Phase 2, the VPN peer or client and the FortiGate unit exchange keys again to establish a secure communication channel. The Phase 2 Proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

Replay Detection

IPsec tunnels can be vulnerable to replay attacks. Replay Detection enables the FortiGate unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the FortiGate unit discards them.

Perfect Forward Secrecy (PFS)

By default, Phase 2 keys are derived from the session key created in Phase 1. Perfect Forward Secrecy (PFS) forces a new Diffie-Hellman exchange when the tunnel starts and whenever the Phase 2 keylife expires, causing a new key to be generated each time. This exchange ensures that the keys created in Phase 2 are unrelated to the Phase 1 keys or any other keys generated automatically in Phase 2.

Keylife

The Keylife setting sets a limit on the length of time that a Phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the Phase 2 key expires, a new key is generated without interrupting service.

Quick mode selectors

Quick mode selectors determine which IP addresses can perform IKE negotiations to establish a tunnel. By only allowing authorized IP addresses access to the VPN tunnel, the network is more secure.

The default settings are as broad as possible: any IP address or configured address object, using any protocol, on any port.

While the drop down menus for specifying an address also show address groups, the use of address groups may not be supported on a remote endpoint device that is not a FortiGate.

The address groups are at the bottom of the list to make it easy to distinguish between addresses and address groups.

When configuring Quick Mode selector **Source address** and **Destination address**, valid options include IPv4 and IPv6 single addresses, IPv4 subnet, or IPv6 subnet. For more information on IPv6 IPsec VPN, see IPv6 IPsec VPNs on page 1717.

There are some configurations that require specific selectors:

- The VPN peer is a third-party device that uses specific phase2 selectors.
- The FortiGate unit connects as a dialup client to another FortiGate unit, in which case (usually) you must specify a source IP address, IP address range, or subnet. However, this is not required if you are using dynamic routing and mode-cfg.

With FortiOS VPNs, your network has multiple layers of security, with quick mode selectors being an important line of defence.

- Routes guide traffic from one IP address to another.
- Phase 1 and Phase 2 connection settings ensure there is a valid remote end point for the VPN tunnel that agrees on the encryption and parameters.
- Quick mode selectors allow IKE negotiations only for allowed peers.
- Security policies control which IP addresses can connect to the VPN.
- Security policies also control what protocols are allowed over the VPN along with any bandwidth limiting.

FortiOS is limited with IKEv2 selector matching. When using IKEv2 with a named traffic selector, no more than 32 subnets per traffic selector are added, since FortiOS doesn't fully implement the IKEv2 selector matching rules.

The workaround is to use multiple Phase 2s. If the configuration is FGT <-> FGT, then the better alternative is to just use 0.0.0.0 <-> 0.0.0.0 and use the firewall policy for enforcement.

Using the add-route option

Consider using the `add-route` option to add a route to a peer destination selector. Phase 2 includes the option of allowing the `add-route` to automatically match the settings in Phase 1. For more information, refer to Phase 1 parameters on page 1581.

Syntax

Phase 2

```
config vpn ipsec {phase2 | phase2-interface}
   edit <name>
      set add-route {phase1 | enable | disable}
   end
end
```

Configuring the Phase 2 parameters

If you are creating a hub-and-spoke configuration or an Internet-browsing configuration, you may have already started defining some of the required Phase 2 parameters. If so, edit the existing definition to complete the configuration.

Specifying the Phase 2 parameters

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Open the **Phase 2 Selectors** panel (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter a **Name** for the Phase 2 configuration, and select a **Phase 1** configuration from the drop-down list.
4. Select **Advanced**.
5. Include the appropriate entries as follows:

Phase 2 Proposal	Select the encryption and authentication algorithms that will be used to change data into encrypted code. Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define. It is invalid to set both **Encryption** and **Authentication** to null.
Encryption	Select a symmetric-key algorithms: **NULL** — Do not use an encryption algorithm. **DES** — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. **3DES** — Triple-DES; plain text is encrypted three times by three keys. **AES128** — A 128-bit block algorithm that uses a 128-bit key. **AES192** — A 128-bit block algorithm that uses a 192-bit key. **AES256** — A 128-bit block algorithm that uses a 256-bit key.

Authentication	You can select either of the following message digests to check the authenticity of messages during an encrypted session: **NULL** — Do not use a message digest. **MD5** — Message Digest 5. **SHA1** — Secure Hash Algorithm 1 - a 160-bit message digest. To specify one combination only, set the **Encryption** and **Authentication** options of the second combination to NULL. To specify a third combination, use the ***Add*** button beside the fields for the second combination. For information regarding NP accelerated offloading of IPsec VPN authentication algorithms, please refer to the Hardware Acceleration handbook chapter.
Enable replay detection	Optionally enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Enable perfect forward secrecy (PFS)	Enable or disable PFS. Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Diffie-Hellman Group	Select one Diffie-Hellman group (1, 2, 5, or 14 through 21). The remote peer or dialup client must be configured to use the same group.
Keylife	Select the method for determining when the Phase 2 key expires: **Seconds**, **KBytes**, or **Both**. If you select **Both**, the key expires when either the time has passed or the number of KB have been processed. The range is from 120 to 172800 seconds, or from 5120 to 2147483648 KB.
Autokey Keep Alive	Enable the option if you want the tunnel to remain active when no data is being processed.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.
DHCP-IPsec	Select **Enable** if the FortiGate unit acts as a dialup server and FortiGate DHCP server or relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP server or relay parameters must be configured separately. If the FortiGate unit acts as a dialup server and the FortiClient dialup client VIP addresses match the network behind the dialup server, select **Enable** to cause the FortiGate unit to act as a proxy for the dialup clients. This is available only for Phase 2 configurations associated with a dialup Phase 1 configuration. It works only on policy-based VPNs.

Autokey Keep Alive

The Phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, however, the SA expires (by default) and the VPN tunnel goes down. A new SA will not be generated until there is traffic.

The Autokey Keep Alive option ensures that a new Phase 2 SA is negotiated, even if there is no traffic, so that the VPN tunnel stays up.

Auto-negotiate

By default, the Phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established. Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.

If the tunnel goes down, the auto-negotiate feature (when enabled) attempts to re-establish the tunnel. Auto-negotiate initiates the Phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.

Automatically establishing the SA can be important for a dialup peer. It ensures that the VPN tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the VPN tunnel does not exist until the dialup peer initiates traffic.

The auto-negotiate feature is available through the Command Line Interface (CLI) via the following commands:

```
config vpn ipsec phase2
   edit <phase2_name>
      set auto-negotiate enable
   end
```

DHCP-IPsec

Select this option if the FortiGate unit assigns VIP addresses to FortiClient dialup clients through a DHCP server or relay. This option is available only if the Remote Gateway in the Phase 1 configuration is set to Dialup User and it works only on policy-based VPNs.

With the DHCP-IPsec option, the FortiGate dialup server acts as a proxy for FortiClient dialup clients that have VIP addresses on the subnet of the private network behind the FortiGate unit. In this case, the FortiGate dialup server acts as a proxy on the local private network for the FortiClient dialup client. When a host on the network behind the dialup server issues an ARP request that corresponds to the device MAC address of the FortiClient host (when a remote server sends an ARP to the local FortiClient dialup client), the FortiGate unit answers the ARP request on behalf of the FortiClient host and forwards the associated traffic to the FortiClient host through the tunnel.

This feature prevents the VIP address assigned to the FortiClient dialup client from causing possible arp broadcast problems — the normal and VIP addresses can confuse some network switches by two addresses having the same MAC address.

Defining VPN security policies

This section explains how to specify the source and destination IP addresses of traffic transmitted through an IPsec VPN, and how to define appropriate security policies.

The following topics are included in this section:

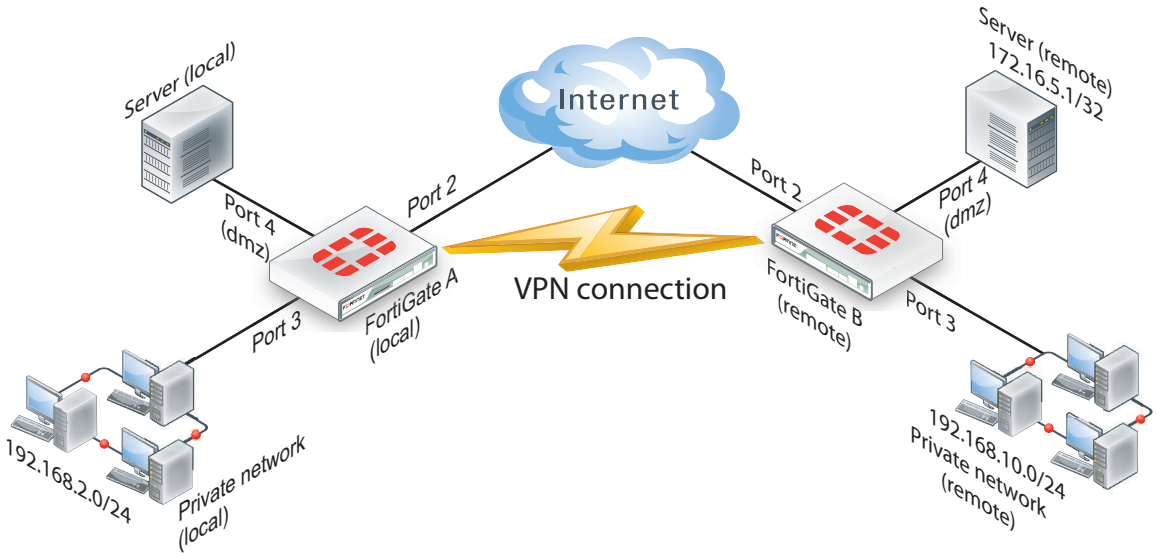
Defining policy addresses
Defining VPN security policies

Defining policy addresses

A VPN tunnel has two end points. These end points may be VPN peers such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the security policy.

Example topology for the following policies



In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer (for example, `192.168.10.0/255.255.255.0` or `192.168.10.0/24`).
- In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer (for example, `172.16.5.1/255.255.255.255` or `172.16.5.1/32` or `172.16.5.1`).

For a FortiGate dialup server in a dialup-client or Internet-browsing configuration:

- If you are not using VIP addresses, or if the FortiGate dialup server assigns VIP addresses to FortiClient dialup clients through FortiGate DHCP relay, select the predefined destination address “all” in the security policy to refer to the dialup clients.
- If you assign VIP addresses to FortiClient dialup clients manually, you need to define a policy address for the VIP address assigned to the dialup client (for example, `10.254.254.1/32`), or a subnet address from which the VIP addresses are assigned (for example, `10.254.254.0/24` or `10.254.254.0/255.255.255.0`).
- For a FortiGate dialup client in a dialup-client or Internet-browsing configuration, you need to define a policy address for the private IP address of a host, server, or network behind the FortiGate dialup server.

To define a security IP address

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. In the **Name** field, type a descriptive name that represents the network, server(s), or host(s).
3. In **Type**, select **Subnet**.
4. In the **Subnet/IP Range** field, type the corresponding IP address and subnet mask.
   For a subnet you could use the format `172.16.5.0/24` or its equivalent `172.16.5.0/255.255.255.0`. For a server or host it would likely be `172.16.5.1/32`. Alternately you can use an IP address range such as `192.168.10.[80-100]` or `192.168.10.80-192.168.10.100`.
5. Select **OK**.

Defining VPN security policies

Security policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source address and destination addresses. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

- A policy-based VPN requires an IPsec security policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.
- A route-based VPN requires an Accept security policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface (Phase 1 configuration) of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.

There are examples of security policies for both policy-based and route-based VPNs throughout this guide. See Dynamic DNS configuration on page 1639.

If the security policy, which grants the VPN Connection is limited to certain services, DHCP must be included, otherwise the client won’t be able to retrieve a lease from the FortiGate’s (IPsec) DHCP server, because the DHCP Request (coming out of the tunnel) will be blocked.

Defining an IPsec security policy for a policy-based VPN

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Allow traffic to be initiated from the remote site

In addition to these operations, security policies specify which IP addresses can initiate a tunnel. by default, traffic from the local private network initiates the tunnel. When the **Allow traffic to be initiated form the remote site** option is selected, traffic from a dialup client or computers on the remote network initiates the tunnel. Both can be enabled at the same time for bi-directional initiation of the tunnel.

Outbound and inbound NAT

When a FortiGate unit operates in NAT mode, you can also enable inbound or outbound NAT. Outbound NAT may be performed on outbound encrypted packets, or on IP packets before they are sent through the tunnel. Inbound NAT is performed on IP packets emerging from the tunnel. By default, these options are not selected in security policies.

When used in conjunction with the `natip` CLI attribute (see the “config firewall” chapter of the FortiGate CLI Reference), outbound NAT enables you to change the source addresses of IP packets before they go into the tunnel. This feature is often used to resolve ambiguous routing when two or more of the private networks making up a VPN have the same or overlapping IP addresses. .

When inbound NAT is enabled, inbound encrypted packets are intercepted and decrypted, and the source IP addresses of the decrypted packets are translated into the IP address of the FortiGate interface to the local private network before they are routed to the private network. If the computers on the local private network can communicate only with devices on the local private network (that is, the FortiGate interface to the private network is not the default gateway) and the remote client (or remote private network) does not have an IP address in the same network address space as the local private network, enable inbound NAT.

Source and destination addresses

Most security policies control outbound IP traffic. A VPN outbound policy usually has a source address originating on the private network behind the local FortiGate unit, and a destination address belonging to a dialup VPN client or a network behind the remote VPN peer. The source address that you choose for the security policy identifies from where outbound cleartext IP packets may originate, and also defines the local IP address or addresses that a remote server or client will be allowed to access through the VPN tunnel. The destination address that you choose identifies where IP packets must be forwarded after they are decrypted at the far end of the tunnel, and determines the IP address or addresses that the local network will be able to access at the far end of the tunnel.

Enabling other policy features

You can fine-tune a policy for services such as HTTP, FTP, and POP3; enable logging, traffic shaping, antivirus protection, web filtering, email filtering, file transfer, and email services throughout the VPN; and optionally allow connections according to a predefined schedule.

As an option, differentiated services (diffserv or DSCP) can be enabled in the security policy through CLI commands. For more information on this feature, see the Traffic Shaping handbook chapter, or the “firewall” chapter of the FortiGate CLI Reference.

When a remote server or client attempts to connect to the private network behind a FortiGate gateway, the security policy intercepts the connection attempt and starts the VPN tunnel. The FortiGate unit uses the remote gateway specified in its Phase 1 tunnel configuration to reply to the remote peer. When the remote peer receives a reply, it checks its own security policy, including the tunnel configuration, to determine which communications are permitted. As long as one or more services are allowed through the VPN tunnel, the two peers begin to

negotiate the tunnel. To follow this negotiation in the web-based manager, go to **VPN > Monitor > IPsec Monitor**. There you will find a list of the VPN tunnels, their status, and the data flow both incoming and outgoing.

Before you begin

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses. See Defining VPN security policies on page 1604.
- Specify the Phase 1 authentication parameters. See Phase 1 parameters on page 1581.
- Specify the Phase 2 parameters. See Phase 2 parameters on page 1598.

To define an IPsec security policy

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New** and set the following options:

Incoming Interface	Select the local interface to the internal (private) network.
Source Address	Select the name that corresponds to the local network, server(s), or host(s) from which IP packets may originate.
Outgoing Interface	Select the local interface to the external (public) network.
Destination Address	Select the name that corresponds to the remote network, server(s), or host (s) to which IP packets may be delivered.
Schedule	Keep the default setting (always) unless changes are needed to meet specific requirements.
Service	Keep the default setting (ANY) unless changes are needed to meet your specific requirements.
Allow traffic to be initiated from the remote site	Select if traffic from the remote network will be allowed to initiate the tunnel.

3. You may enable UTM features, and/or event logging, or select advanced settings to authenticate a user group, or shape traffic. For more information, see the Firewall handbook chapter.
4. Select **OK**.
5. Place the policy in the policy list above any other policies having similar source and destination addresses.

Defining multiple IPsec policies for the same tunnel

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPsec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY security policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list. When you define multiple IPsec policies for the same tunnel, you must reorder the IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

Adding multiple IPsec policies for the same VPN tunnel can cause conflicts if the policies specify similar source and destination addresses but have different settings for the same service. When policies overlap in this manner, the system may apply the wrong IPsec policy or the tunnel may fail.

For example, if you create two equivalent IPsec policies for two different tunnels, it does not matter which one comes first in the list of IPsec policies — the system will select the correct policy based on the specified source and destination addresses. If you create two different IPsec policies for the same tunnel (that is, the two policies treat traffic differently depending on the nature of the connection request), you might have to reorder the IPsec policies to ensure that the system selects the correct IPsec policy. Reordering is especially important when the source and destination addresses in both policies are similar (for example, if one policy specifies a subset of the IP addresses in another policy). In this case, place the IPsec policy having the most specific constraints at the top of the list so that it can be evaluated first.

Defining security policies for a route-based VPN

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary Accept security policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPsec security policies.

To define security policies for a route-based VPN

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New** and leave the **Policy Type** as **Firewall**, and the **Policy Subtype** as **Address**.
3. Define an ACCEPT security policy to permit communications between the local private network and the private network behind the remote peer. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select the address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select the IPsec Interface you configured.
Destination Address	Select the address name that you defined for the private network behind the remote peer.
Action	Select **ACCEPT**.
Enable NAT	Disable.

To permit the remote client to initiate communication, you need to define a security policy for communication in that direction.

4. Select **Create New** and leave the **Policy Type** as **Firewall**, and the **Policy Subtype** as **Address**
5. Enter these settings in particular:

Incoming Interface	Select the IPsec Interface you configured.

Source Address	Select the address name that you defined for the private network behind the remote peer.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select the address name that you defined for the private network behind this FortiGate unit.
Action	Select ***ACCEPT***.
Enable NAT	Disable.

Gateway-to-gateway configurations

This section explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN.

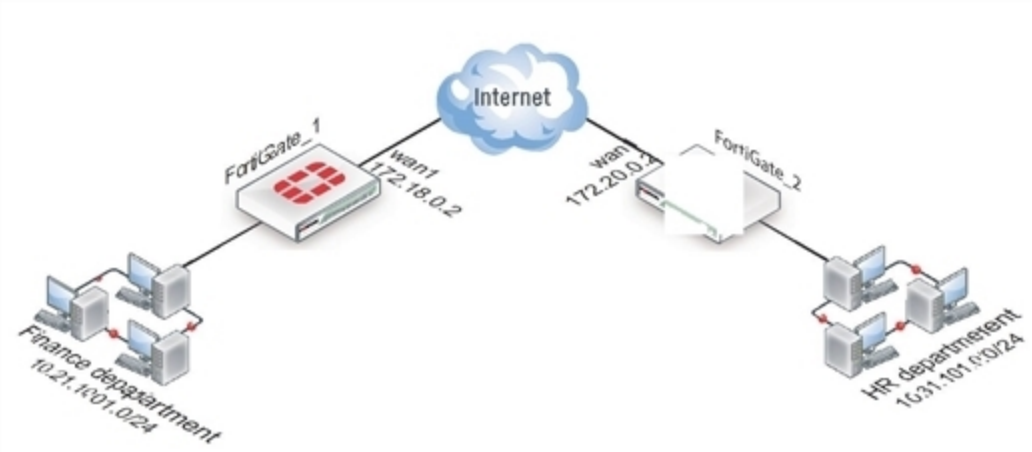
The following topics are included in this section:

Configuration overview
General configuration steps
Configuring the two VPN peers
How to work with overlapping subnets
Testing

Configuration overview

In a gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks. All traffic between the two networks is encrypted and protected by FortiGate security policies.

Example gateway-to-gateway configuration

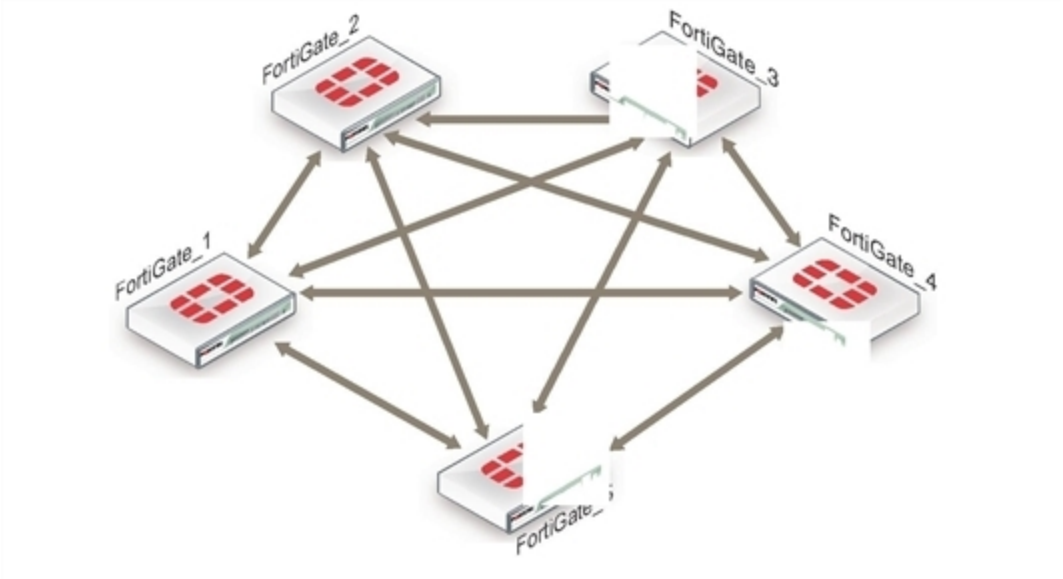


In some cases, computers on the private network behind one VPN peer may (by co-incidence) have IP addresses that are already used by computers on the network behind the other VPN peer. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and traffic destined for the remote network through the tunnel may not be sent. To resolve issues related to ambiguous routing, see Configuration overview on page 1609.

In other cases, computers on the private network behind one VPN peer may obtain IP addresses from a local DHCP server. However, unless the local and remote networks use different private network address spaces, unintended ambiguous routing and/or IP-address overlap issues may arise. For a discussion of the related issues, see FortiGate dialup-client configurations on page 1669.

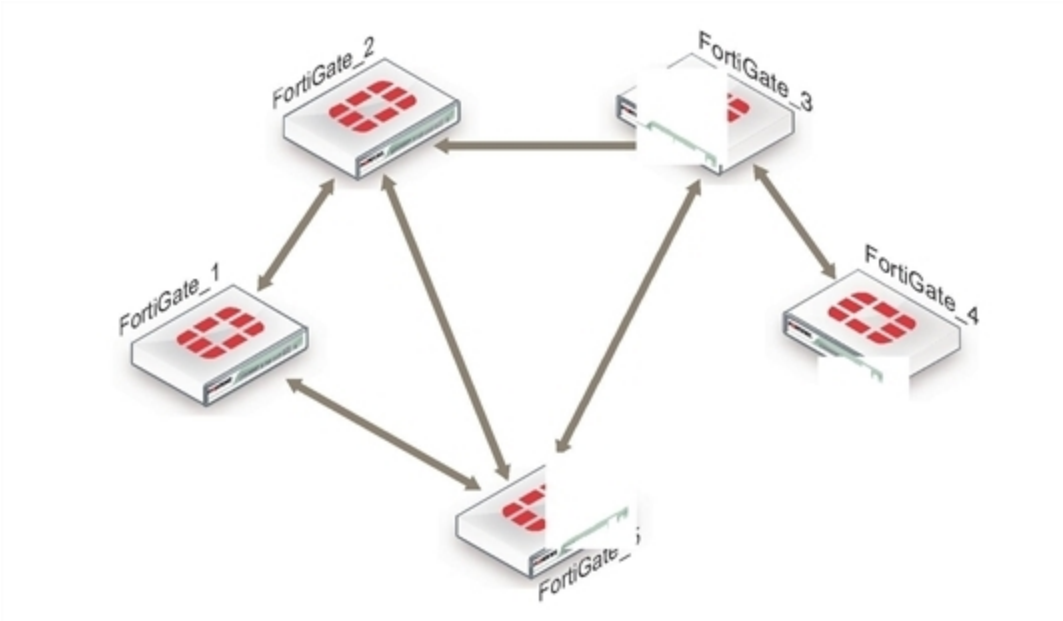
You can set up a fully meshed or partially meshed configuration (see below).

Fully meshed configuration



In a fully meshed network, all VPN peers are connected to each other, with one hop between peers. This topology is the most fault-tolerant: if one peer goes down, the rest of the network is not affected. This topology is difficult to scale because it requires connections between all peers. In addition, unnecessary communication can occur between peers. Best practices dictates a hub-and-spoke configuration instead (see Hub-and-spoke configurations on page 1623).

Partially meshed configuration



A partially meshed network is similar to a fully meshed network, but instead of having tunnels between all peers, tunnels are only configured between peers that communicate with each other regularly.

General configuration steps

The FortiGate units at both ends of the tunnel must be operating in NAT mode and have static public IP addresses.

When a FortiGate unit receives a connection request from a remote VPN peer, it uses IPsec Phase 1 parameters to establish a secure connection and authenticate that VPN peer. Then, if the security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec Phase 2 parameters and applies the IPsec security policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed by both FortiGate units:

- Define the Phase 1 parameters that the FortiGate unit needs to authenticate the remote peer and establish a secure connection.
- Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.
- Create security policies to control the permitted services and permitted direction of traffic between the IP source and destination addresses.

Configuring the two VPN peers

Configure the VPN peers as follows. Each step is required, but these are general steps. For more detailed information on each step follow the cross references. See Phase 1 parameters on page 1581. All steps are required. Cross references point to required information that is repeated. No steps are optional.

Configuring Phase 1 and Phase 2 for both peers

This procedure applies to both peers. Repeat the procedure on each FortiGate unit, using the correct IP address for each. You may wish to vary the Phase 1 names but this is optional. Otherwise all steps are the same for each peer.

The Phase 1 configuration defines the parameters that FortiGate_1 will use to authenticate FortiGate_2 and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate FortiGate_2. The same preshared key must be specified at both FortiGate units.

Before you define the Phase 1 parameters, you need to:

- Reserve a name for the remote gateway.
- Obtain the IP address of the public interface to the remote peer.
- Reserve a unique value for the preshared key.

The key must contain at least 6 printable characters and best practices dictate that it only be known by network administrators. For optimum protection against currently known attacks, the key must have a minimum of 16 randomly chosen alphanumeric characters.

At the local FortiGate unit, define the Phase 1 configuration needed to establish a secure connection with the remote peer. See IPsec VPN in the web-based manager on page 1568.

To create Phase 1 to establish a secure connection with the remote peer

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**.

Name	Enter `peer_1`. A name to identify the VPN tunnel. This name appears in Phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select **Static IP Address**.
IP Address	Enter `172.20.0.2` when configuring FortiGate_1. Enter `172.18.0.2` when configuring FortiGate_2. The IP address of the remote peer public interface.
Local Interface	Select **wan1**.

The basic Phase 2 settings associate IPsec Phase 2 parameters with the Phase 1 configuration and specify the remote end point of the VPN tunnel. Before you define the Phase 2 parameters, you need to reserve a name for the tunnel. See IPsec VPN in the web-based manager on page 1568.

To configure Phase 2 settings

1. Open the **Phase 2 Selectors** panel (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
2. Enter a **Name** of `peer_1_p2`.
3. Select **peer_1** from the **Phase 1** drop-down menu.

Creating security policies

Security policies control all IP traffic passing between a source address and a destination address.

An IPsec security policy is needed to allow the transmission of encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. A single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define security policies, you must first specify the IP source and destination addresses. In a gateway-to-gateway configuration:

- The IP source address corresponds to the private network behind the local FortiGate unit.
- The IP destination address refers to the private network behind the remote VPN peer.

When you are creating security policies, choose one of either route-based or policy-based methods and follow it for both VPN peers. DO NOT configure both route-based and policy-based policies on the same FortiGate unit for the same VPN tunnel.

The configuration of FortiGate_2 is similar to that of FortiGate_1. You must:

- Define the Phase 1 parameters that FortiGate_2 needs to authenticate FortiGate_1 and establish a secure connection.
- Define the Phase 2 parameters that FortiGate_2 needs to create a VPN tunnel with FortiGate_1.
- Create the security policy and define the scope of permitted services between the IP source and destination addresses.

When creating security policies it is good practice to include a comment describing what the policy does.

When creating security policies you need to be

- Creating firewall addresses
- Creating route-based VPN security policies
- Configuring a default route for VPN interface

or

- Creating firewall addresses
- Creating policy-based VPN security policy

Creating firewall addresses

Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the security policies that permit communication between the networks.

To define the IP address of the network behind FortiGate_1

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Enter the **Name** of `Finance_network`.
3. Select a **Type** of **Subnet**.
4. Enter the **Subnet** of `10.21.101.0/24`.
5. Select **OK**.

To specify the address of the network behind FortiGate_2

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Enter the **Name** of `HR_network`.
3. Select a **Type** of **Subnet**.
4. Enter the **Subnet/IP Range** of `10.31.101.0/24`.
5. Select **OK**.

Creating route-based VPN security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses.

To create route-based VPN security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following, and select **OK**.

Incoming Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.

Source Address	Select **Finance_network** when configuring FortiGate_1. Select **HR_network** when configuring FortiGate_2. The address name for the private network behind this FortiGate unit.
Outgoing Interface	Select **peer_1**. The VPN Tunnel (IPsec Interface) you configured earlier.
Destination Address	Select **HR_network** when configuring FortiGate_1. Select **Finance_network** when configuring FortiGate_2. The address name that you defined for the private network behind the remote peer.
Action	Select **ACCEPT**.
Enable NAT	Disable.
Comments	Allow Internal to remote VPN network traffic.

4. Optionally, configure any additional features you may want, such as UTM or traffic shaping.
5. Select **Create New** to create another policy for the other direction.
6. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
7. Enter the following information, and select **OK**.

Incoming Interface	Select **peer_1**. The VPN Tunnel (IPsec Interface) you configured.
Source Address	Select **HR_network** when configuring FortiGate_1. Select **Finance_Network** when configuring FortiGate_2. The address name defined for the private network behind the remote peer.
Outgoing Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.
Destination Address	Select **Finance_Network** when configuring FortiGate_1. Select **HR_network** when configuring FortiGate_2. The address name defined for the private network behind this FortiGate unit.
Action	Select **ACCEPT**.

Enable NAT	Disable.
Comments	Allow remote VPN network traffic to Internal.

8. Configure any additional features such as UTM or traffic shaping you may want. (optional).

Configuring a default route for VPN interface

All network traffic must have a static route to direct its traffic to the proper destination. Without a route, traffic will not flow even if the security policies are configured properly. You may need to create a static route entry for both directions of VPN traffic if your security policies allow bi-directional tunnel initiation.

To configure the route for a route-based VPN

1. On FortiGate_2, go to **Router > Static > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the following information, and then select **OK**:

Destination IP / Mask	10.21.101.0/24
Device	FGT2_to_FGT1_Tunnel
Gateway	Leave as default: 0.0.0.0.
Distance (Advanced)	Leave this at its default. If there are other routes on this FortiGate unit, you may need to set the distance on this route so the VPN traffic will use it as the default route. However, this normally happens by default because this route is typically a better match than the generic default route.

Creating policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Complete the following:

Incoming Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.
Source Address	Select **Finance_network** when configuring FortiGate_1. Select **HR_network** when configuring FortiGate_2. The address name defined for the private network behind this FortiGate unit.

Outgoing Interface	Select **wan1**. The FortiGate unit's public interface.
Destination Address	Select **HR_network** when configuring FortiGate_1. Select **Finance_network** when configuring FortiGate_2.
VPN Tunnel	Select **Use Existing** and select **peer_1** from the **VPN Tunnel** drop-down list. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.
Comments	Bidirectional policy-based VPN policy.

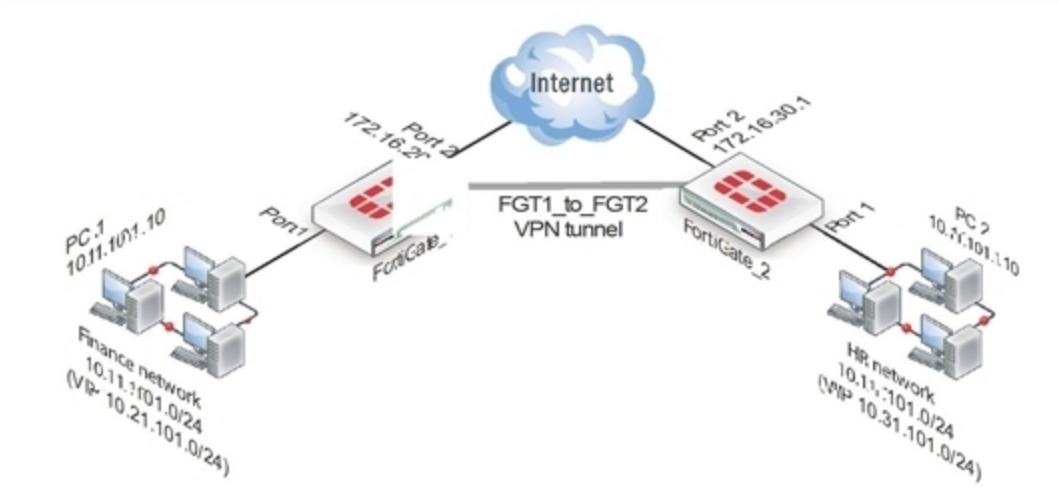
Place VPN policies in the policy list above any other policies having similar source and destination addresses.

How to work with overlapping subnets

A site-to-site VPN configuration sometimes has the problem that the private subnet addresses at each end are the same. You can resolve this problem by remapping the private addresses using virtual IP addresses (VIP).

VIPs allow computers on those overlapping private subnets to each have another set of IP addresses that can be used without confusion. The FortiGate unit maps the VIP addresses to the original addresses. This means if PC1 starts a session with PC2 at 10.31.101.10, FortiGate_2 directs that session to 10.11.101.10 — the actual IP address of PC2.The figure below demonstrates this — Finance network VIP is 10.21.101.0/24 and the HR network is 10.31.101.0/24.

Overlapped subnets example



Solution for route-based VPN

You need to:

- Configure IPsec Phase 1 and Phase 2 as you usually would for a route-based VPN. In this example, the resulting IPsec interface is named `FGT1_to_FGT2`.
- Configure virtual IP (VIP) mapping:
  - the 10.21.101.0/24 network mapped to the 10.11.101.0/24 network on FortiGate_1
  - the 10.31.101.0/24 network mapped to the 10.11.101.0/24 network on FortiGate_2
- Configure an outgoing security policy with ordinary source NAT on both FortiGates.
- Configure an incoming security policy with the VIP as the destination on both FortiGates.
- Configure a route to the remote private network over the IPsec interface on both FortiGates.

To configure VIP mapping on both FortiGates

1. Go to **Policy & Objects > Objects > Virtual IPs** and select **Create New**.
2. Enter the following information, and select **OK**:

Name	Enter a name, for example, `my_vip`.
External Interface	Select `FGT1_to_FGT2`. The IPsec interface.
Type	Static NAT
External IP Address/Range	For the **External IP Address** field enter: `10.21.101.1` when configuring FortiGate_1, or `10.31.101.1` when configuring FortiGate_2.
Mapped IP Address/Range	For the **Mapped IP Address** enter `10.11.101.1`. For the **Range** enter `10.11.101.254`.
Port Forwarding	Disable

3. Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the outbound security policy on both FortiGates

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and select **OK**:

Incoming Interface	Select **Port 1**.
Source Address	Select **all**.
Outgoing Interface	Select **FGT1_to_FGT2**. The IPsec interface.
Destination Address	Select **all**.
Action	Select **ACCEPT**

Enable NAT	Enable

4. Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the inbound security policy on both FortiGates

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and then select **OK**:

Incoming Interface	Select **FGT1_to_FGT2**.
Source Address	Select **all**.
Outgoing Interface	Select **Port 1**. The IPsec interface.
Destination Address	Select **my-vip**.
Action	Select **ACCEPT**
Enable NAT	Disable

4. Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the static route for both FortiGates

1. Go to **Router > Static > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the following information, and then select **OK**:

Destination IP / Mask	Enter `10.31.101.0/24 when` configuring FortiGate_1. Enter `10.21.101.0/24` when configuring FortiGate_2.
Device	Select **FGT1_to_FGT2**.
Gateway	Leave as default: 0.0.0.0.
Distance (Advanced)	Leave at default. If you have advanced routing on your network, you may have to change this value

Solution for policy-based VPN

As with the route-based solution, users contact hosts at the other end of the VPN using an alternate subnet address. PC1 communicates with PC2 using IP address 10.31.101.10, and PC2 communicates with PC1 using IP address 10.21.101.10.

In this solution however, outbound NAT is used to translate the source address of packets from the 10.11.101.0/24 network to the alternate subnet address that hosts at the other end of the VPN use to reply. Inbound packets from the remote end have their destination addresses translated back to the 10.11.101.0/24 network.

For example, PC1 uses the destination address 10.31.101.10 to contact PC2. Outbound NAT on FortiGate_1 translates the PC1 source address to 10.21.101.10. At the FortiGate_2 end of the tunnel, the outbound NAT configuration translates the destination address to the actual PC2 address of 10.11.101.10. Similarly, PC2 replies to PC1 using destination address 10.21.101.10, with the PC2 source address translated to 10.31.101.10. PC1 and PC2 can communicate over the VPN even though they both have the same IP address.

- You need to:
- Configure IPsec Phase 1 as you usually would for a policy-based VPN.
- Configure IPsec Phase 2 with the `use-natip disable` CLI option.
- Define a firewall address for the local private network, 10.11.101.0/24.
- Define a firewall address for the remote private network:
  - Define a firewall address for 10.31.101.0/24 on FortiGate_1
  - Define a firewall address for 10.21.101.0/24 on FortiGate_2
- Configure an outgoing IPsec security policy with outbound NAT to map 10.11.101.0/24 source addresses:
  - To the 10.21.101.0/24 network on FortiGate_1
  - To the 10.31.101.0/24 network on FortiGate_2

To configure IPsec Phase 2 - CLI

```
config vpn ipsec phase2
   edit "FGT1_FGT2_p2"
      set keepalive enable
      set pfs enable
      set phase1name FGT1_to_FGT2
      set proposal 3des-sha1 3des-md5
      set replay enable
      set use-natip disable
   end
```

In this example, your Phase 1 definition is named FGT1_to_FGT2. `use-natip` is set to `disable`, so you can specify the source selector using the **`src-addr-type`**, `src-start-ip` / `src-end-ip` or `src-subnet` keywords. This example leaves these keywords at their default values, which specify the subnet `0.0.0.0/0`.

The `pfs` keyword ensures that perfect forward secrecy (PFS) is used. This ensures that each Phase 2 key created is unrelated to any other keys in use.

To define the local private network firewall address

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Enter the following information and select **OK**.

Name	Enter `vpn-local`. A meaningful name for the local private network.
Type	Subnet
Subnet / IP Range	10.11.101.0 255.255.255.0
Interface	Any

To define the remote private network firewall address

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Enter the following information, and select **OK**:

Name	Enter `vpn-remote`. A meaningful name for the remote private network.
Type	Subnet
Subnet / IP Range	`10.31.101.0 255.255.255.0` on FortiGate_1. `10.21.101.0 255.255.255.0` on FortiGate_2.
Interface	Any

To configure the IPsec security policy

In the CLI on FortiGate_1, enter the commands:

```
config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "vpn-local"
      set dstaddr "vpn-remote"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "FGT1_to_FGT2"
      set natoutbound enable
      set natip 10.31.101.0 255.255.255.0
   end
```

Optionally, you can set everything except `natip` in the web-based manager and then use the CLI to set `natip`.

Enter the same commands on FortiGate_2, but set natip be `10.21.101.0 255.255.255.0`.

Testing

The best testing is to look at the packets both as the VPN tunnel is negotiated, and when the tunnel is up.

To determine what the other end of the VPN tunnel is proposing

1. Start a terminal program such as puTTY and set it to log all output.

   When necessary refer to the logs to locate information when output is verbose.
2. Logon to the FortiGate unit using a super_admin account.
3. Enter the following CLI commands.
4. Display all the possible IKE error types and the number of times they have occurred:
   ```
   diag vpn ike errors
   ```
5. Check for existing debug sessions:
   ```
   diag debug info
   ```

If a debug session is running, to halt it enter:

```
diag debug disable
```

6. Confirm your proposal settings:
```
diag vpn ike config list
```
7. If your proposal settings do not match what you expect, make a change to it and save it to force an update in memory. If that fixes the problem, stop here.
8. List the current vpn filter:
```
diag vpn ike filter
```
9. If all fields are set to any, there are no filters set and all VPN IKE packets will be displayed in the debug output. If your system has only a few VPNs, skip setting the filter.

   If your system has many VPN connections this will result in very verbose output and make it very difficult to locate the correct connection attempt.
10. Set the VPN filter to display only information from the destination IP address for example 10.10.10.10:
```
diag vpn ike log-filter dst-addr4 10.10.10.10
```
    To add more filter options, enter them one per line as above. Other filter options are:

clear	erase the current filter
dst-addr6	the IPv6 destination address range to filter by
dst-port	the destination port range to filter by
interface	interface that IKE connection is negotiated over
list	display the current filter
name	the phase1 name to filter by
negate	negate the specified filter parameter
src-addr4	the IPv4 source address range to filter by
src-addr6	the IPv6 source address range to filter by
src-port	the source port range to filter by
vd	index of virtual domain. 0 matches all

11. Start debugging:
```
diag debug app ike 255
diag debug enable
```
12. Have the remote end attempt a VPN connection.

    If the remote end attempts the connection they become the initiator. This situation makes it easier to debug VPN tunnels because then you have the remote information and all of your local information. by initiate the connection, you will not see the other end's information.
13. If possible go to the web-based manager on your FortiGate unit, go to the VPN monitor and try to bring the tunnel up.
14. Stop the debug output:
```
diag debug disable
```

15. Go back through the output to determine what proposal information the initiator is using, and how it is different from your VPN P1 proposal settings.

Things to look for in the debug output of attempted VPN connections are shown below.

Important terms to look for in VPN debug output

`initiator`	Starts the VPN attempt, in the above procedure that is the remote end
`responder`	Answers the initiator's request
`local ID`	In aggressive mode, this is not encrypted
`error no SA proposal chosen`	There was no proposal match — there was no encryption-authentication pair in common, usually occurs after a long list of proposal attempts
`R U THERE and R U THERE ack`	dead peer detection (dpd), also known as dead gateway detection — after three failed attempts to contact the remote end it will be declared dead, no farther attempts will be made to contact it
`negotiation result`	lists the proposal settings that were agreed on
`SA_life_soft and SA_life_hard`	negotiating a new key, and the key life
`R U THERE`	If you see this, it means Phase 1 was successful
`tunnel up`	the negotiation was successful, the VPN tunnel is operational

Hub-and-spoke configurations

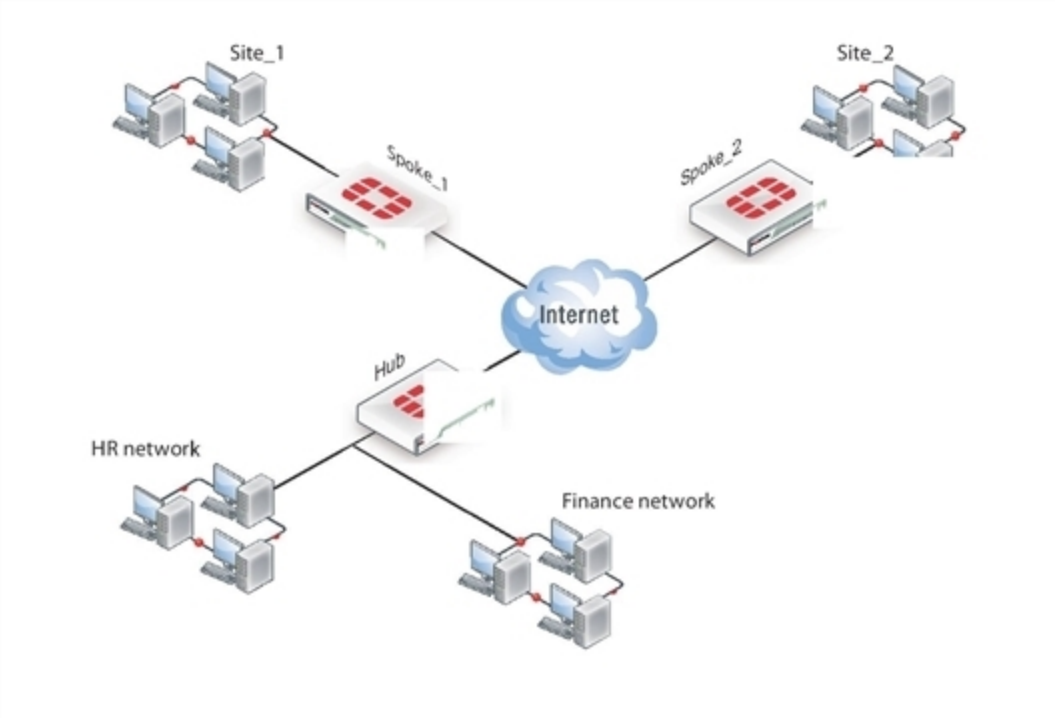
This section describes how to set up hub-and-spoke IPsec VPNs. The following topics are included in this section:

Configuration overview
Configure the hub
Configure the spokes
Dynamic spokes configuration example

Configuration overview

In a hub-and-spoke configuration, VPN connections radiate from a central FortiGate unit (the hub) to a number of remote peers (the spokes). Traffic can pass between private networks behind the hub and private networks behind the remote peers. Traffic can also pass between remote peer private networks through the hub.

Example hub-and-spoke configuration



The actual implementation varies in complexity depending on:

- Whether the spokes are statically or dynamically addressed
- The addressing scheme of the protected subnets
- How peers are authenticated

This guide discusses the issues involved in configuring a hub-and-spoke VPN and provides some basic configuration examples.

Hub-and-spoke infrastructure requirements

- The FortiGate hub must be operating in NAT mode and have a static public IP address.
- Spokes may have static IP addresses, dynamic IP addresses (see FortiGate dialup-client configurations on page 1669), or static domain names and dynamic IP addresses (see Dynamic DNS configuration on page 1639).

Spoke gateway addressing

The public IP address of the spoke is the VPN remote gateway as seen from the hub. Statically addressed spokes each require a separate VPN Phase 1 configuration on the hub. When there are many spokes, this becomes rather cumbersome.

Using dynamic addressing for spokes simplifies the VPN configuration because then the hub requires only a single Phase 1 configuration with “dialup user” as the remote gateway. You can use this configuration even if the remote peers have static IP addresses. A remote peer can establish a VPN connection regardless of its IP address if its traffic selectors match and it can authenticate to the hub. See Configuration overview on page 1623 for an example of this configuration.

Protected networks addressing

The addresses of the protected networks are needed to configure destination selectors and sometimes for security policies and static routes. The larger the number of spokes, the more addresses there are to manage. You can

- Assign spoke subnets as part of a larger subnet, usually on a new network

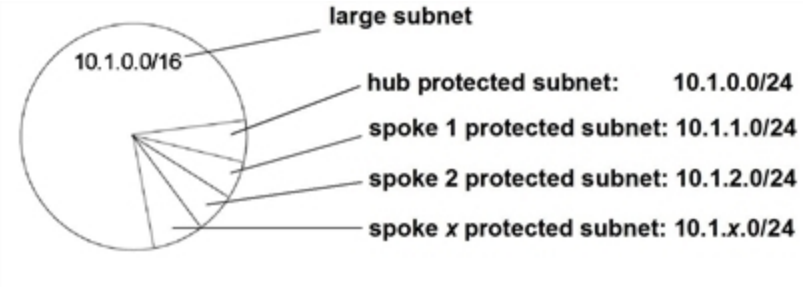
  or

- Create address groups that contain all of the needed addresses

Using aggregated subnets

If you are creating a new network, where subnet IP addresses are not already assigned, you can simplify the VPN configuration by assigning spoke subnets that are part of a large subnet.

Aggregated subnets



All spokes use the large subnet address, 10.1.0.0/16 for example, as:

- The IPsec destination selector
- The destination of the security policy from the private subnet to the VPN (required for policy-based VPN, optional for route-based VPN)
- The destination of the static route to the VPN (route-based)

Each spoke uses the address of its own protected subnet as the IPsec source selector and as the source address in its VPN security policy. The remote gateway is the public IP address of the hub FortiGate unit.

Using an address group

If you want to create a hub-and-spoke VPN between existing private networks, the subnet addressing usually does not fit the aggregated subnet model discussed earlier. All of the spokes and the hub will need to include the addresses of all the protected networks in their configuration.

On FortiGate units, you can define a named firewall address for each of the remote protected networks and add these addresses to a firewall address group. For a policy-based VPN, you can then use this address group as the destination of the VPN security policy.

For a route-based VPN, the destination of the VPN security policy can be set to All. You need to specify appropriate routes for each of the remote subnets.

Authentication

Authentication is by a common pre-shared key or by certificates. For simplicity, the examples in this chapter assume that all spokes use the same pre-shared key.

Configure the hub

At the FortiGate unit that acts as the hub, you need to:

- Configure the VPN to each spoke
- Configure communication between spokes

You configure communication between spokes differently for a policy-based VPN than for a route-based VPN. For a policy-based VPN, you configure a VPN concentrator. For a route-based VPN, you must either define security policies or group the IPsec interfaces into a zone

Define the hub-spoke VPNs

Perform these steps at the FortiGate unit that will act as the hub. Although this procedure assumes that the spokes are all FortiGate units, a spoke could also be VPN client software, such as FortiClient Endpoint Security.

To configure the VPN hub

1. At the hub, define the Phase 1 configuration for each spoke. See Phase 1 parameters on page 1581. Enter these settings in particular:

Name	Enter a name to identify the VPN in Phase 2 configurations, security policies and the VPN monitor.

Remote Gateway	The remote gateway is the other end of the VPN tunnel. There are three options: **Static IP Address** — Enter the spoke's public **IP Address**. You will need to create a Phase 1 configuration for each spoke. Either the hub or the spoke can establish the VPN connection. **Dialup User** — No additional information is needed. The hub accepts connections from peers with appropriate encryption and authentication settings. Only one Phase 1 configuration is needed for multiple dialup spokes. Only the spoke can establish the VPN tunnel. **Dynamic DNS** — If the spoke subscribes to a dynamic DNS service, enter the spoke's **Dynamic DNS** domain name. Either the hub or the spoke can establish the VPN connection. For more information, see Dynamic DNS configuration on page 1639.
Local Interface	Select the FortiGate interface that connects to the remote gateway. This is usually the FortiGate unit's public interface.

2. Define the Phase 2 parameters needed to create a VPN tunnel with each spoke. See Phase 2 parameters on page 1598. Enter these settings in particular:

Name	Enter a name to identify this spoke Phase 2 configuration.
Phase 1	Select the name of the Phase 1 configuration that you defined for this spoke.

Define the hub-spoke security policies

1. Define a name for the address of the private network behind the hub. For more information, see Defining VPN security policies on page 1603.
2. Define names for the addresses or address ranges of the private networks behind the spokes. For more information, see Defining VPN security policies on page 1603.
3. Define the VPN concentrator. See To define the VPN concentrator on page 1628.
4. Define security policies to permit communication between the hub and the spokes. For more information, see Defining VPN security policies on page 1603.

Route-based VPN security policies

Define ACCEPT security policies to permit communications between the hub and the spoke. You need one policy for each direction.

To add policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured in Step 1.
Source Address	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.
Outgoing Interface	Select the hub's interface to the internal (private) network.
Destination Address	Select the source address that you defined in Step 1.
Action	Select **ACCEPT**.
Enable NAT	Enable.

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured inStep 1.
Source Address	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate units.
Outgoing Interface	Select the source address that you defined in Step 1.
Destination Address	Select the hub's interface to the internal (private) network.
Action	Select **ACCEPT**.
Enable NAT	Enable.

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the hub and the spoke.

To add policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter these settings in particular:

Incoming Interface	Select the hub's interface to the internal (private) network.
Source Address	Select the source address that you defined in Step 1.
Outgoing Interface	Select the hub's public network interface.
Destination Address	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration that you created for the spoke in Step 1. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

In the policy list, arrange the policies in the following order:

- IPsec policies that control traffic between the hub and the spokes first
- The default security policy last

Configuring communication between spokes (policy-based VPN)

For a policy-based hub-and-spoke VPN, you define a concentrator to enable communication between the spokes.

To define the VPN concentrator

1. At the hub, go to **VPN > IPsec > Concentrator** and select **Create New**.
2. In the **Concentrator Name** field, type a name to identify the concentrator.
3. From the **Available Tunnels** list, select a VPN tunnel and then select the right-pointing arrow.
4. Repeat Step 3 until all of the tunnels associated with the spokes are included in the concentrator.
5. Select **OK**.

Configuring communication between spokes (route-based VPN)

For a route-based hub-and-spoke VPN, there are several ways you can enable communication between the spokes:

- Put all of the IPsec interfaces into a zone and enable intra-zone traffic. This eliminates the need for any security policy for the VPN, but you cannot apply UTM features to scan the traffic for security threats.
- Put all of the IPsec interfaces into a zone and create a single zone-to-zone security policy
- Create a security policy for each pair of spokes that are allowed to communicate with each other. The number of policies required increases rapidly as the number of spokes increases.

Using a zone as a concentrator

A simple way to provide communication among all of the spokes is to create a zone and allow intra-zone communication. You cannot apply UTM features using this method.

1. Go to **System > Network > Interfaces**.
2. Select the down-arrow on the **Create New** button and select **Zone**.
3. In the **Zone Name** field, enter a name, such as `Our_VPN_zone`.
4. Clear **Block intra-zone traffic**.
5. In the **Interface Members** list, select the IPsec interfaces that are part of your VPN.
6. Select **OK**.

Using a zone with a policy as a concentrator

If you put all of the hub IPsec interfaces involved in the VPN into a zone, you can enable communication among all of the spokes and apply UTM features with just one security policy.

To create a zone for the VPN

1. Go to **System > Network > Interfaces**.
2. Select the down-arrow on the **Create New** button and select **Zone**.
3. In the **Zone Name** field, enter a name, such as `Our_VPN_zone`.
4. Select **Block intra-zone traffic**.

5. In the **Interface Members** list, select the IPsec interfaces that are part of your VPN.
6. Select **OK**.

To create a security policy for the zone

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the settings: and select **OK**.

Incoming Interface	Select the zone you created for your VPN.
Source Address	Select ***All***.
Outgoing Interface	Select the zone you created for your VPN.
Destination Address	Select ***All***.
Action	Select **ACCEPT**.
Enable NAT	Enable.

Using security policies as a concentrator

To enable communication between two spokes, you need to define an ACCEPT security policy for them. To allow either spoke to initiate communication, you must create a policy for each direction. This procedure describes a security policy for communication from Spoke 1 to Spoke 2. Others are similar.

1. Define names for the addresses or address ranges of the private networks behind each spoke. For more information, see Defining VPN security policies on page 1603.
2. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
3. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
4. Enter the settings and select **OK**.

Incoming Interface	Select the IPsec interface that connects to Spoke 1.
Source Address	Select the address of the private network behind Spoke 1.
Outgoing Interface	Select the IPsec interface that connects to Spoke 2.
Destination Address	Select the address of the private network behind Spoke 2.
Action	Select **ACCEPT**.
Enable NAT	Enable.

Configure the spokes

Although this procedure assumes that the spokes are all FortiGate units, a spoke could also be VPN client software, such as FortiClient Endpoint Security.

Perform these steps at each FortiGate unit that will act as a spoke.

To create the Phase 1 and phase_2 configurations

1. At the spoke, define the Phase 1 parameters that the spoke will use to establish a secure connection with the hub. See Phase 1 parameters on page 1581. Enter these settings:

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the interface that connects to the hub.

2. Create the Phase 2 tunnel definition. See Phase 2 parameters on page 1598. Select the set of Phase 1 parameters that you defined for the hub. You can select the name of the hub from the **Static IP Address** part of the list.

Configuring security policies for hub-to-spoke communication

1. Create an address for this spoke. See Defining VPN security policies on page 1603. Enter the IP address and netmask of the private network behind the spoke.
2. Create an address to represent the hub. See Defining VPN security policies on page 1603. Enter the IP address and netmask of the private network behind the hub.
3. Define the security policy to enable communication with the hub.

Route-based VPN security policy

Define two security policies to permit communications to and from the hub.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings:

Incoming Interface	Select the virtual IPsec interface you created.
Source Address	Select the hub address you defined in Step 1.
Outgoing Interface	Select the spoke's interface to the internal (private) network.
Destination Address	Select the spoke addresses you defined in Step 2.
Action	Select **ACCEPT**.
Enable NAT	Enable

Incoming Interface	Select the spoke's interface to the internal (private) network.
Source Address	Select the spoke address you defined in Step 1.
Outgoing Interface	Select the virtual IPsec interface you created.
Destination Address	Select the hub destination addresses you defined in Step 2.

Action	Select **ACCEPT**.
Enable NAT	Enable

Policy-based VPN security policy

Define an IPsec security policy to permit communications with the hub. See Defining VPN security policies on page 1603.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter these settings in particular:

Incoming Interface	Select the spoke's interface to the internal (private) network.
Source Address	Select the spoke address you defined in Step 1.
Outgoing Interface	Select the spoke's interface to the external (public) network.
Destination Address	Select the hub address you defined in Step 2.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration you defined. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

Configuring security policies for spoke-to-spoke communication

Each spoke requires security policies to enable communication with the other spokes. Instead of creating separate security policies for each spoke, you can create an address group that contains the addresses of the networks behind the other spokes. The security policy then applies to all of the spokes in the group.

1. Define destination addresses to represent the networks behind each of the other spokes. Add these addresses to an address group.
2. Define the security policy to enable communication between this spoke and the spokes in the address group you created.

Policy-based VPN security policy

Define an IPsec security policy to permit communications with the other spokes. See Defining VPN security policies on page 1603. Enter these settings in particular:

Route-based VPN security policy

Define two security policies to permit communications to and from the other spokes.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the virtual IPsec interface you created.
Source Address	Select the spoke address group you defined in Step "Configure the spokes " on page 1629.
Outgoing Interface	Select the spoke's interface to the internal (private) network.
Destination Address	Select this spoke's address name.
Action	Select **ACCEPT**.
Enable NAT	Enable

4. Select **Create New**, leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**, and enter these settings:

Incoming Interface	Select the spoke's interface to the internal (private) network.
Source Address	Select this spoke's address name.
Outgoing Interface	Select the virtual IPsec interface you created.
Destination Address	Select the spoke address group you defined in Step 1.
Action	Select **ACCEPT**.
Enable NAT	Enable

Policy-based VPN security policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following:

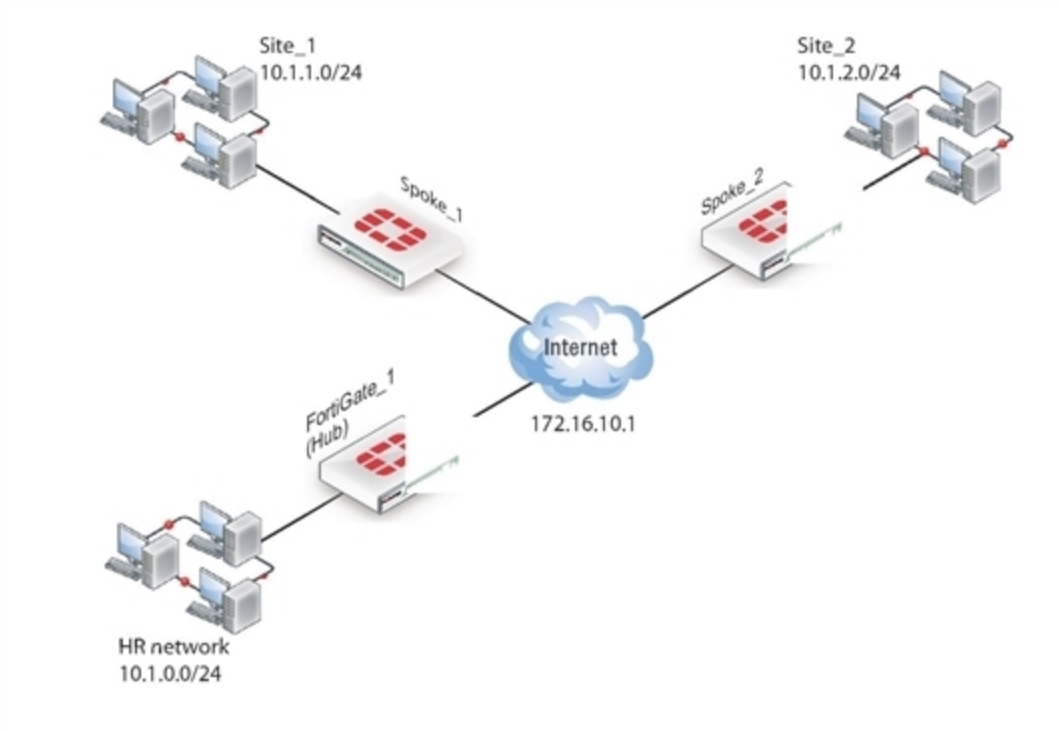
Incoming Interface	Select this spoke's internal (private) network interface.
Source Address	Select this spoke's source address.
Outgoing Interface	Select the spoke's interface to the external (public) network.
Destination Address	Select the spoke address group you defined in Step 1.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration you defined. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

Place this policy or policies in the policy list above any other policies having similar source and destination addresses.

Dynamic spokes configuration example

This example demonstrates how to set up a basic route-based hub-and-spoke IPsec VPN that uses preshared keys to authenticate VPN peers.

Example hub-and-spoke configuration



In the example configuration, the protected networks 10.1.0.0/24, 10.1.1.0/24 and 10.1.2.0/24 are all part of the larger subnet 10.1.0.0/16. The steps for setting up the example hub-and-spoke configuration create a VPN among Site 1, Site 2, and the HR Network.

The spokes are dialup. Their addresses are not part of the configuration on the hub, so only one spoke definition is required no matter the number of spokes. For simplicity, only two spokes are shown.

Configure the hub (FortiGate_1)

The Phase 1 configuration defines the parameters that FortiGate_1 will use to authenticate spokes and establish secure connections.

For the purposes of this example, one preshared key will be used to authenticate all of the spokes. Each key must contain at least 6 printable characters and best practices dictates that it only be known by network administrators. For optimum protection against currently known attacks, each key must consist of a minimum of 16 randomly chosen alphanumeric characters.

Define the IPsec configuration

To define the Phase 1 parameters

1. At FortiGate_1, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button). Define the Phase 1 parameters that the hub will use to establish a secure connection to the spokes.

Name	Enter a name (for example, `toSpokes`).
Remote Gateway	Dialup user
Local Interface	External
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID

The basic Phase 2 settings associate IPsec Phase 2 parameters with the Phase 1 configuration and specify the remote end points of the VPN tunnels.

To define the Phase 2 parameters

1. Open the **Phase 2 Selectors** panel (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
2. Enter the following information, and select **OK**:

Name	Enter a name for the Phase 2 definition (for example, `toSpokes_ph2`).
Phase 1	Select the Phase 1 configuration that you defined previously (for example, `toSpokes`).

Define the security policies

security policies control all IP traffic passing between a source address and a destination address. For a route-based VPN, the policies are simpler than for a policy-based VPN. Instead of an IPSEC policy, you use an ACCEPT policy with the virtual IPsec interface as the external interface.

Before you define security policies, you must first define firewall addresses to use in those policies. You need addresses for:

- The HR network behind FortiGate_1
- The aggregate subnet address for the protected networks

To define the IP address of the HR network behind FortiGate_1

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, enter the following information, and select **OK**:

Name	Enter an address name (for example, `HR_Network`).
Type	Subnet
Subnet/IP Range	Enter the IP address of the HR network behind FortiGate_1 (for example, `10.1.0.0/24`).

To specify the IP address the aggregate protected subnet

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, enter the following information, and select **OK**:

Address Name	Enter an address name (for example, `Spoke_net`).
Type	Subnet
Subnet/IP Range	Enter the IP address of the aggregate protected network, `10.1.0.0/16`

To define the security policy for traffic from the hub to the spokes

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**,
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and select **OK**:

Incoming Interface	Select the interface to the HR network, **port 1**.
Source Address	`Select` **HR_Network**.
Outgoing Interface	Select the virtual IPsec interface that connects to the spokes, `toSpokes`.
Destination Address	`Select` **Spoke_net**.
Action	Select **ACCEPT**.

Place the policy in the policy list above any other policies having similar source and destination addresses.

Configure communication between spokes

Spokes communicate with each other through the hub. You need to configure the hub to allow this communication. An easy way to do this is to create a zone containing the virtual IPsec interfaces even if there is only one, and create a zone-to-zone security policy.

To create a zone for the VPN

1. Go to **System > Network > Interfaces**.
2. Select the down-arrow on the **Create New** button and select **Zone**.
3. In the **Zone Name** field, enter a name, such as `Our_VPN_zone`.
4. Select **Block intra-zone traffic**.
   You could enable intra-zone traffic and then you would not need to create a security policy. But, you would not be able to apply UTM features.

5. In **Interface Members**, select the virtual IPsec interface, `toSpokes`.
6. Select **OK**.

To create a security policy for the zone

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings:

Incoming Interface	Select `Our_VPN_zone`.
Source Address	Select **All**.
Outgoing Interface	Select `Our_VPN_zone`.
Destination Address	Select **All**.
Action	Select **ACCEPT**.
Enable NAT	Enable.

4. Select **OK**.

Configure the spokes

In this example, all spokes have nearly identical configuration, requiring the following:

- Phase 1 authentication parameters to initiate a connection with the hub.
- Phase 2 tunnel creation parameters to establish a VPN tunnel with the hub.
- A source address that represents the network behind the spoke. This is the only part of the configuration that is different for each spoke.
- A destination address that represents the aggregate protected network.
- A security policy to ena.ble communications between the spoke and the aggregate protected network

Define the IPsec configuration

At each spoke, create the following configuration.

To define the Phase 1 parameters

1. At the spoke, go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button). Enter the following information:

Name	Type a name, for example, `toHub`.
Remote Gateway	Select **Static IP Address**.
IP Address	Enter `172.16.10.1`.

Local Interface	Select **Port2**.
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate_1 configuration
Peer Options	Select **Any peer ID**.

To define the Phase 2 parameters

1. Open the **Phase 2 Selectors** panel (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
2. Enter the following information and select **OK**:

Name	Enter a name for the tunnel, for example, `toHub_ph2`.
Phase 1	Select the name of the Phase 1 configuration that you defined previously, for example, `toHub`.
Advanced	Select to show the following **Quick Mode Selector** settings.
Source	Enter the address of the protected network at this spoke. For spoke_1, this is `10.1.1.0/24`. For spoke_2, this is `10.1.2.0/24`.
Destination	Enter the aggregate protected subnet address, `10.1.0.0/16`.

Define the security policies

You need to define firewall addresses for the spokes and the aggregate protected network and then create a security policy to enable communication between them.

To define the IP address of the network behind the spoke

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New** and enter the following information:

Address Name	Enter an address name, for example `LocalNet`.
Type	Subnet
Subnet/IP Range	Enter the IP address of the private network behind the spoke. For spoke_1, this is `10.1.1.0/24`. For spoke_2, this is `10.1.2.0/24`.

To specify the IP address of the aggregate protected network

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New** and enter the following information:

Address Name	Enter an address name, for example, `Spoke_net`.
Type	Subnet
Subnet/IP Range	Enter the IP address of the aggregate protected network, `10.1.0.0/16`.

To define the security policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information:

Incoming Interface	Select the virtual IPsec interface, `toHub`.
Source Address	Select the aggregate protected network address `Spoke_net`.
Outgoing Interface	Select the interface to the internal (private) network, `port1`.
Destination Address	Select the address for this spoke's protected network `LocalNet`.
Action	Select **ACCEPT**.

4. Select **Create New**.
5. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
6. Enter the following information, and select **OK**:

Incoming Interface	Select the interface to the internal private network, `port1`.
Source Address	Select the address for this spoke's protected network, `LocalNet`.
Outgoing Interface	Select the virtual IPsec interface, `toHub`.
Destination Address	Select the aggregate protected network address, `Spoke_net`.
Action	Select **ACCEPT**.

Place these policies in the policy list above any other policies having similar source and destination addresses.

Dynamic DNS configuration

This section describes how to configure a site-to-site VPN, in which one FortiGate unit has a static IP address and the other FortiGate unit has a domain name and a dynamic IP address.

The following topics are included in this section:

Dynamic DNS over VPN concepts
Dynamic DNS topology
General configuration steps
Configure the dynamically-addressed VPN peer
Configure the fixed-address VPN peer
Testing

Dynamic DNS over VPN concepts

A typical computer has a static IP address and one or more DNS servers to resolve fully qualified domain names (FQDN) into IP addresses. A domain name assigned to this computer is resolved by any DNS server having an entry for the domain name and its static IP address. The IP address never changes or changes only rarely so the DNS server can reliably say it has the correct address for that domain all the time.

Dynamic DNS (DDNS)

It is different when a computer has a dynamic IP address, such as an IP address assigned dynamically by a DHCP server, and a domain name. Computers that want to contact this computer do not know what its current IP address is. To solve this problem there are dynamic DNS servers. These are public servers that store a DNS entry for your computer that includes its current IP address and associated domain name. These entries are kept up to date by your computer sending its current IP address to the dynamic DNS (DDNS) server to ensure its entry is always up to date. When other computers want to contact your domain, their DNS gets your IP address from your DDNS server. To use DDNS servers, you must subscribe to them and usually pay for their services.

When configuring DDNS on your FortiGate unit, go to **System > Network > DNS** and enable **Enable FortiGuard DDNS**. Then select the interface with the dynamic connection, which DDNS server you have an account with, your domain name, and account information. If your DDNS server is not on the list, there is a generic option where you can provide your DDNS server information.

Routing

When an interface has some form of changing IP address (DDNS, PPPoE, or DHCP assigned address), routing needs special attention. The standard static route cannot handle the changing IP address. The solution is to use the dynamic-gateway command in the CLI. Say for example you already have four static routes, and you have a PPPoE connection over the wan2 interface and you want to use that as your default route.

The route is configured on the dynamic address VPN peer trying to access the static address FortiGate unit.

To configure dynamic gateway routing - CLI

```
config router static
   edit 5
      set dst 0.0.0.0 0.0.0.0
```

```
        set dynamic-gateway enable
        set device wan2
    next
end
```

For more information on DDNS, see the System Administration handbook chapter.

Dynamic DNS over VPN

IPsec VPN expects an IP address for each end of the VPN tunnel. All configuration and communication with that tunnel depends on the IP addresses as reference points. However, when the interface the tunnel is on has DDNS enabled there is no set IP address. The remote end of the VPN tunnel now needs another way to reference your end of the VPN tunnel. This is accomplished using Local ID.

A FortiGate unit that has a domain name and a dynamic IP address can initiate VPN connections anytime. The remote peer can reply to the local FortiGate unit using the source IP address that was sent in the packet header because it is current. Without doing a DNS lookup first, the remote peer runs the risk of the dynamic IP changing before it attempts to connect. To avoid this, the remote peer must perform a DNS lookup for the domain name of to be sure of the dynamic IP address before initiating the connection.

Remote Gateway

When configuring the Phase 1 entry for a VPN tunnel, the Remote Gateway determines the addressing method the remote end of the tunnel uses as one of Static IP Address, Dialup User, or Dynamic DNS. There are different fields for each option.

When you select the Dynamic DNS VPN type there is a related field called Dynamic DNS. The Dynamic DNS field is asking for the FQDN of the remote end of the tunnel. It uses this information to look up the IP address of the remote end of the tunnel through the DDNS server associated with that domain name.

Local ID (peer ID)

The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel. This enables a more secure connection. Also if you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure it on your end, it is your Local ID. When the remote end connects to you, they see it as your peer ID.

If you are debugging a VPN connection, the Local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.

To configure your Local ID

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Select **Advanced**.
4. In the **Phase 1 Proposal** section, enter your Local ID.
5. Select **OK**.

The default configuration is to accept all local IDs (peer IDs). If you have the Local ID set, the remote end of the tunnel must be configured to accept your Local ID.

To accept a specific Peer ID

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Select **Aggressive** mode.
4. For **Peer Options**, select **This peer ID**. This option becomes visible only when Aggressive mode is selected.
5. Enter the string the other end of the tunnel used for its Local ID.
6. Configure the rest of the Phase 1 entry as required.
7. Select **OK**.

Route-based or policy-based VPN

VPN over dynamic DNS can be configured with either route-based or policy-based VPN settings. Both are valid, but have differences in configuration. Choose the best method based on your requirements. For more information on route-based and policy-based, see IPsec VPN overview on page 1563.

Route-based VPN configuration requires two security policies to be configured (one for each direction of traffic) to permit traffic over the VPN virtual interface, and you must also add a static route entry for that VPN interface or the VPN traffic will not reach its destination. See Dynamic DNS over VPN concepts on page 1639 and Dynamic DNS over VPN concepts on page 1639.

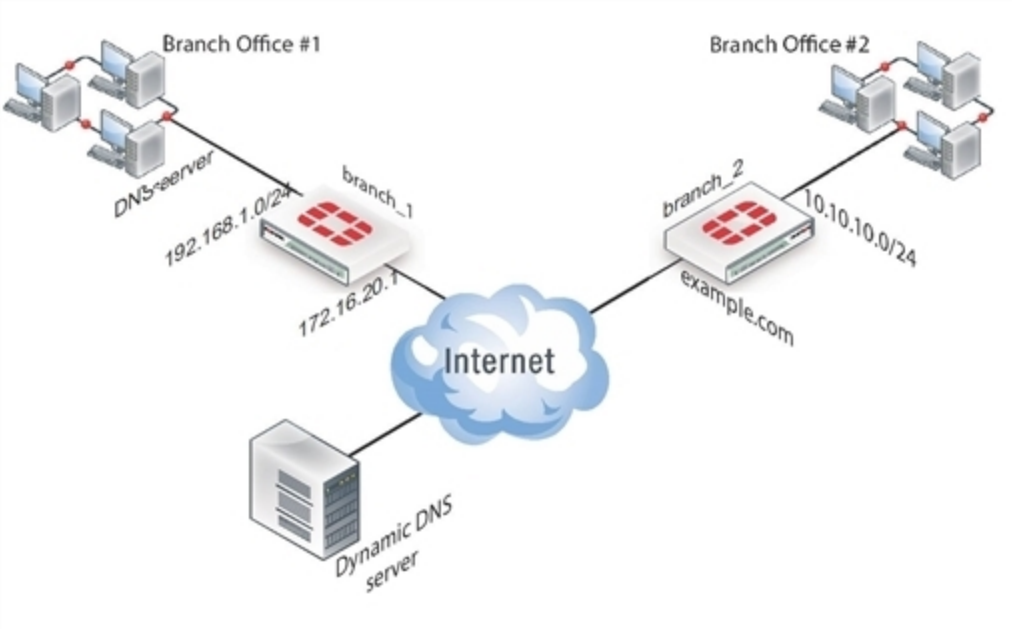
Policy-based VPN configuration uses more complex and often more IPsec security policies, but does not require a static route entry. It has the benefit of being able to configure multiple policies for handling multiple protocols in different ways, such as more scanning of less secure protocols or guaranteeing a minimum bandwidth for protocols such as VoIP. See Dynamic DNS over VPN concepts on page 1639 and Dynamic DNS over VPN concepts on page 1639.

Dynamic DNS topology

In this scenario, two branch offices each have a FortiGate unit and are connected in a gateway-to-gateway VPN configuration. One FortiGate unit has a domain name (example.com) with a dynamic IP address. See `branch_2` in the figure below.

Whenever the `branch_2` unit connects to the Internet (and possibly also at predefined intervals set by the ISP), the ISP may assign a different IP address to the FortiGate unit. The unit has its domain name registered with a dynamic DNS service. The `branch_2` unit checks in with the DDNS server on a regular basis, and that server provides the DNS information for the domain name, updating the IP address from time to time. Remote peers have to locate the `branch_2` FortiGate unit through a DNS lookup each time to ensure the address they get is current and correct.

Example dynamic DNS configuration



When a remote peer (such as the `branch_1` FortiGate unit above) initiates a connection to `example.com`, the local DNS server looks up and returns the IP address that matches the domain name `example.com`. The remote peer uses the retrieved IP address to establish a VPN connection with the `branch_2` FortiGate unit.

Assumptions

- You have administrator access to both FortiGate units.
- Both FortiGate units have interfaces named wan1 and internal. (If not, you can use the alias feature to assign these labels as “nicknames” to other interfaces to follow this example.)
- Both FortiGate units have the most recent firmware installed, have been configured for their networks, and are currently passing normal network traffic.
- The `branch_2` FortiGate unit has its `wan1` interface defined as a dynamic DNS interface with the domain name of **example.com**.
- A basic gateway-to-gateway configuration is in place (see Gateway-to-gateway configurations on page 1609) except one of the FortiGate units has a static domain name and a dynamic IP address instead of a static IP address.
- The FortiGate unit with the domain name is subscribed to one of the supported dynamic DNS services. Contact one of the services to set up an account. For more information and instructions about how to configure the FortiGate unit to push its dynamic IP address to a dynamic DNS server, see the System Administration handbook chapter.

General configuration steps

When a FortiGate unit receives a connection request from a remote VPN peer, it uses IPsec Phase 1 parameters to establish a secure connection and authenticate the VPN peer. Then, if the security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec Phase 2 parameters and applies the security policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

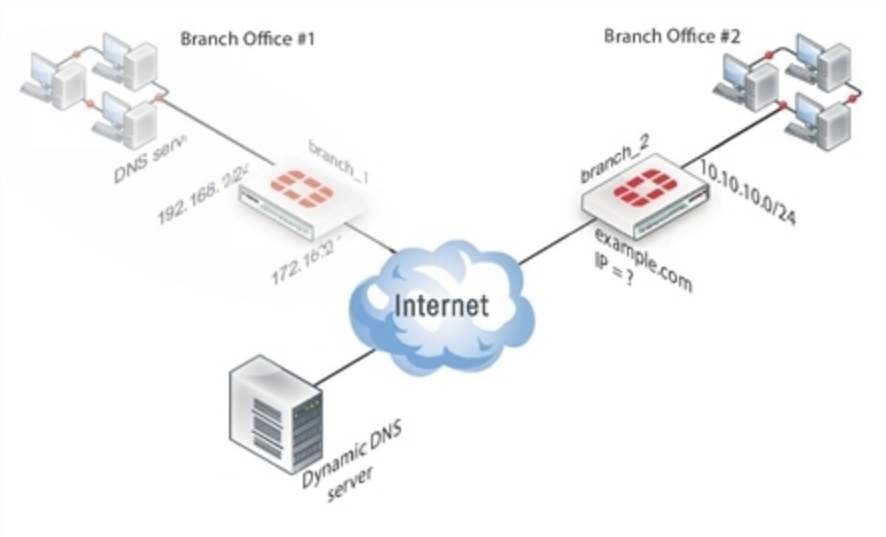
To support these functions, the following general configuration steps must be performed:

- Configure the branch_2 FortiGate unit with the dynamic IP address. This unit uses a Local ID string instead of an IP address to identify itself to the remote peer. See General configuration steps below.
  - General configuration steps
  - General configuration steps
- Configure the fixed-address VPN peer. To initiate a VPN tunnel with the dynamically-addressed peer, this unit must first retrieve the IP address for the domain from the dynamic DNS service. See General configuration steps on page 1643.
  - General configuration steps
  - General configuration steps

Configure the dynamically-addressed VPN peer

It is assumed that this FortiGate unit (`branch_2`) has already had its public facing interface, for example the `wan1`, configured with the proper dynamic DNS configuration.

Configure branch_2, the dynamic address side



Configuring the dynamically-addressed VPN peer includes:

- Configuring branch_2 VPN tunnel settings
- Configuring branch_2 security policies

Configuring branch_2 VPN tunnel settings

Define the Phase 1 parameters needed to establish a secure connection with the remote peer. See Phase 1 parameters on page 1581. During this procedure you need to choose if you will be using route-based or policy-based VPNs.

To configure branch_2 VPN tunnel settings

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information:

Name	Enter `branch_2`, a name to identify the VPN tunnel. This name appears in Phase 2 configurations, security policies, and the VPN monitor.
Remote Gateway	Select **Static IP Address**. The remote peer this FortiGate is connecting to has a static IP public address. If the remote interface is PPPoE do not select **Retrieve default gateway from server**.
IP Address	Enter `172.16.20.1`. The IP address of the public interface to the remote peer.

Enter 172.16.20.1 The IP address of the public interface to the remote peer.	Select **Aggressive**.

4. Select **Advanced** and complete the following:

Local ID	Enter `example.com`. A character string used by the `branch_2` FortiGate unit to identify itself to the remote peer. This value must be identical to the value in the **This peer ID** field of the Phase 1 remote gateway configuration on the branch_1 remote peer. See Configure the dynamically-addressed VPN peer on page 1643.

5. Open the **Phase 2 Selectors** panel.

   Define the Phase 2 parameters needed to create a VPN tunnel with the remote peer. For details on Phase 2, see Phase 2 parameters on page 1598.
6. Enter the following information and select **OK**.

Name	Enter `branch_2_phase2`. A name to identify this Phase 2 configuration.
Phase 1	Select `branch_2`. The name of the Phase 1 configuration that you defined earlier.

Configuring branch_2 security policies

Define security policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see Defining VPN security policies on page 1603.

After defining the two address ranges, select one of Creating branch_2 route-based security policies on page 1646 or Creating branch_2 policy-based security policies on page 1648 to configure the appropriate VPN policies.

Define address ranges for branch_2 security policies

Define VPN connection names for the address ranges of the private networks. These addresses are used in the security policies that permit communication between the networks. For more information, see Defining VPN security policies on page 1603.

Define an address name for the IP address and netmask of the private network behind the local FortiGate unit.

To define branch_2 address ranges

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**.

3. Enter the following information, and select **OK**.

Name	Enter `branch_2_internal`. Enter a meaningful name.
Type	Select **Subnet**.
Subnet / IP Range	Enter `10.10.10.0/24`. Include the netmask or specify a specific range.
Interface	Select **internal**. The interface that will be handling the traffic from the internal network.

Define an address name for the IP address and netmask of the private network behind the remote peer.

4. Select **Create New**.
5. Enter the following information, and select **OK**.

Name	Enter `branch_1_internal`. A meaningful name for the private network at the remote end of the VPN tunnel.
Type	Select **Subnet**.
Subnet / IP Range	Enter `192.168.1.0/24`. Include the netmask. Optionally you can specify a range
Interface	Select **any**. The interface that will be handling the remote VPN traffic on this FortiGate unit. If you are unsure, or multiple interfaces may be handling this traffic use `any`.

Creating branch_2 route-based security policies

Define ACCEPT security policies to permit communication between the branch_2 and branch_1 private networks. Once the route-based policy is configured a routing entry must be configured to route traffic over the VPN interface.

Define a policy to permit the branch_2 local FortiGate unit to initiate a VPN session with the branch_1 VPN peer.

To create route-based security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and select **OK**.

Incoming Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.
Source Address	Select **branch_2_internal**. Select the address name for the private network behind this FortiGate unit.
Outgoing Interface	Select **branch_2**. The VPN Tunnel (IPsec Interface).
Destination Address	Select **branch_1_internal**. The address name the private network behind the remote peer.
Action	Select ***ACCEPT***.
Enable NAT	Disable.
Comments	Route-based: Initiate a branch_2 to branch_1 VPN tunnel.

Define a policy to permit the branch_1 remote VPN peer to initiate VPN sessions.

4. Select **Create New**.
5. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
6. Enter the following information, and select **OK**.

Incoming Interface	Select **branch_2**. The VPN Tunnel (IPsec Interface).
Source Address	Select **branch_1_internal**. The address name for the private network behind the remote peer.
Outgoing Interface	Select **internal**. The interface connecting the private network behind this FortiGate unit.
Destination Address	Select **branch_2_internal**. The address name for the private network behind this FortiGate unit.
Action	Select ***ACCEPT***.
Enable NAT	Disable.
Comments	Route-based: Initiate a branch_1 to branch_2 internal VPN tunnel.

7. Optionally configure any other security policy settings you require such as UTM or traffic shaping for this policy.
8. Place these policies in the policy list above any other policies having similar source and destination addresses. This will ensure VPN traffic is matched against the VPN policies before any other policies.

To create routing entry for VPN interface - CLI

```
config router static
   edit 5
      set dst 0.0.0.0 0.0.0.0
      set dynamic-dateway enable
```

```
        set device wan1
    next
end
```

This routing entry must be added in the CLI because the dynamic-gateway option is not available in the web-based manager.

Creating branch_2 policy-based security policies

Define an IPsec policy to permit VPN sessions between the private networks. Define an IPsec policy to permit the VPN sessions between the local branch_2 unit and the remote branch_1 unit.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**.

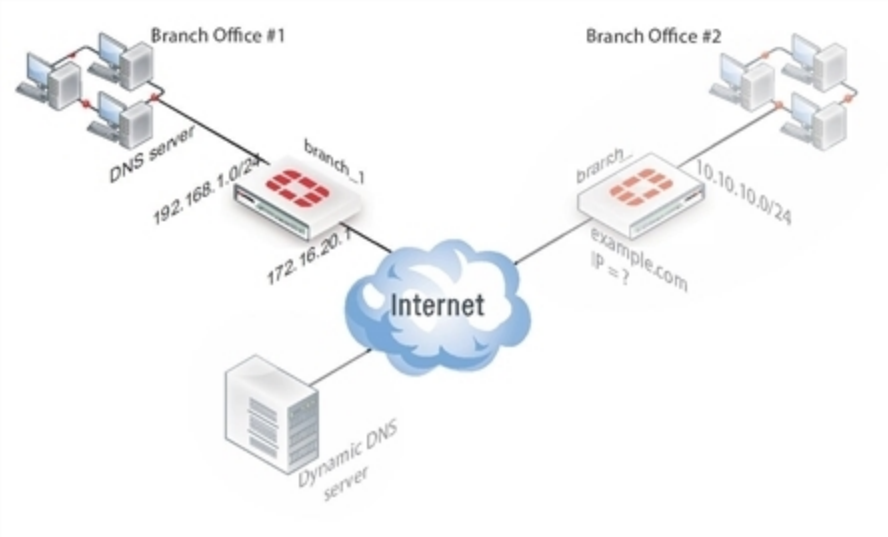
Incoming Interface	Select **internal**. The interface connecting the private network behind this FortiGate unit.
Source Address	Select **branch_2_internal**. The address name for the private network behind this local FortiGate unit.
Outgoing Interface	Select **wan1**. The FortiGate unit's public interface.
Destination Address	Select **branch_1_internal**. The address name for the private network behind branch_1, the remote peer.
VPN Tunnel	Select **Use Existing** and select **branch_2** from the drop-down list. The name of the Phase 1 tunnel.
	Select **Allow traffic to be initiated from the remote site**.
Comments	Policy-based: allows traffic in either direction to initiate the VPN tunnel.

3. Optionally configure any other security policy settings you require such as UTM or traffic shaping for this policy.
4. Place these policies in the policy list above any other policies having similar source and destination addresses. This will ensure VPN traffic is matched against the VPN policies before any other policies.

Configure the fixed-address VPN peer

The fixed-address VPN peer, branch_1, needs to retrieve the IP address from the dynamic DNS service to initiate communication with the dynamically-addressed peer, branch_2. It also depends on the peer ID (local ID) to initiate the VPN tunnel with branch_2.

Configure branch_1, the fixed address side



Configuring the fixed-address VPN peer includes:

- Configuring branch_1 VPN tunnel settings
- Configuring branch_1 security policies

Configuring branch_1 VPN tunnel settings

Define the Phase 1 parameters needed to establish a secure connection with the remote peer. For more information, see Phase 1 parameters on page 1581.

To configure branch_1 Phase 1 VPN settings

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information and select **OK**.

Name	Enter `branch_1`. A name to identify the VPN tunnel. This name appears in Phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select **Dynamic DNS**. The remote peer this FortiGate is connecting to has a dynamic IP address.
Dynamic DNS	Type the fully qualified domain name of the remote peer (for example, `example.com`).
Interface	Select **wan1**. The public facing interface on the fixed-address FortiGate unit.
Mode	Select **Aggressive**.
Peer Options	Select **This peer ID**, and enter `example.com`. This option only appears when the mode is set to Aggressive. The identifier of the FortiGate unit with the dynamic address.

4. Define the Phase 2 parameters needed to create a VPN tunnel with the remote peer. See Phase 2 parameters on page 1598. Enter these settings in particular:

Name	Enter `branch_1_p2`. A name to identify this Phase 2 configuration.
Phase 1	Select **branch_1**. The name of the Phase 1 configuration that you defined for the remote peer. You can select the name of the remote gateway from the Dynamic DNS part of the list.

Configuring branch_1 security policies

The `branch_1` FortiGate unit has a fixed IP address and will be connecting to the `branch_2` FortiGate unit that has a dynamic IP address and a domain name of `example.com`. Remember if you are using route-based security policies that you must add a route for the VPN traffic.

Defining address ranges for branch_1 security policies

As with `branch_2` previously, `branch_1` needs address ranges defined as well. See Defining VPN security policies on page 1603.

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**.
3. Enter the following information, and select **OK**.

Name	Enter `branch_2_internal`. A meaningful name for the private network behind the `branch_2` FortiGate unit.
Type	Select **Subnet**.
Subnet / IP Range	Enter `10.10.10.0/24`. Include the netmask or specify a specific range.
Interface	Select **internal**. This is the interface on this FortiGate unit that will be handling with this traffic.

4. Define an address name for the IP address and netmask of the private network behind the remote peer.
5. Select **Create New**.
6. Enter the following information, and select **OK**.

Name	Enter `branch_1_internal`. A meaningful name for the private network behind the `branch_1` peer.
Type	Select **Subnet**.
Subnet / IP Range	Enter `192.168.1.0/24`. Include the netmask or specify a specific range.
Interface	Select **any**. The interface on this FortiGate unit that will be handling with this traffic. If you are unsure, or multiple interfaces may be handling this traffic use `any`.

Creating branch_1 route-based security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses. See Defining VPN security policies on page 1603.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and select **OK**.

Incoming Interface	Select **internal**. The interface that connects to the private network behind the `branch_1` FortiGate unit.
Source Address	Select **branch_1_internal**. The address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select **branch_1**. The VPN Tunnel (IPsec Interface) you configured earlier.
Destination Address	Select **branch_2_internal**. The address name that you defined for the private network behind the `branch_2` peer.
Action	Select **ACCEPT**.
Enable NAT	Disable
Comments	Internal -> branch2

To permit the remote client to initiate communication, you need to define a security policy for communication in that direction.

4. Select **Create New**.
5. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
6. Enter the following information, and select **OK**.

Incoming Interface	Select **branch_1**. The VPN Tunnel (IPsec Interface) you configured earlier.
Source Address	Select **branch_2_internal**. The address name that you defined for the private network behind the `branch_2` remote peer.
Outgoing Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.
Destination Address	Select **branch_1_internal**. The address name that you defined for the private network behind this FortiGate unit.
Action	Select **ACCEPT**.
Enable NAT	Disable
Comments	branch_2 -> Internal

Creating branch_1 policy-based security policies

A policy-based security policy allows you the flexibility to allow inbound or outbound traffic or both through this single policy.

This policy-based IPsec VPN security policy allows both inbound and outbound traffic

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**.

Incoming Interface	Select **internal**. The interface that connects to the private network behind this FortiGate unit.
Source Address	Select **branch_1_internal**. The address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select **wan1**. The FortiGate unit's public interface.
Destination Address	Select **branch_2_internal**. The address name that you defined for the private network behind the remote peer.
VPN Tunnel	Select **Use Existing** and select **branch_1** from the drop-down list. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

3. Place this security policy in the policy list above any other policies having similar source and destination addresses.

Testing

Once both ends are configured, you can test the VPN tunnel.

To test the VPN initiated by branch_2

1. On branch_2, go to **VPN > Monitor > IPsec Monitor**.
   All IPsec VPN tunnels will be listed on this page, no matter if they are connected or disconnected.
2. Select the tunnel listed for branch_2, and select the status column for that entry.
   The status will say **Bring Up** and remote port, incoming and outgoing data will all be zero. This indicates an inactive tunnel. When you select **Bring Up**, the FortiGate will try to set up a VPN session over this tunnel. If it is successful, Bring Up will change to Active, and the arrow icon will change to a green up arrow icon.
3. If this does not create a VPN tunnel with increasing values for incoming and outgoing data, you need to start troubleshooting:

To test the VPN initiated by branch_1

1. On branch_1, go to **VPN > Monitor > IPsec Monitor**.
2. Select the tunnel listed for branch_1, and select the status column.
   The difference between branch_2 and branch_1 at this point is that the tunnel entry for branch-1 will not have a remote gateway IP address. It will be resolved when the VPN tunnel is started.

3. If this does not create a VPN tunnel with increasing values for incoming and outgoing data, you need to start troubleshooting.

Some troubleshooting ideas include:

- If there was no entry for the tunnel on the monitor page, check the Auto Key (IKE) page to verify the Phase 1 and Phase 2 entries exist.
- Check the security policy or policies, and ensure there is an outgoing policy as a minimum.
- Check that you entered a local ID in the Phase 1 configuration, and that branch_1 has the same local ID.
- Ensure the local DNS server has an up-to-date DNS entry for exmaple.com.

For more information on VPN troubleshooting and testing, see Logging and monitoring on page 1769.

FortiClient dialup-client configurations

The FortiClient Endpoint Security application is an IPsec VPN client with antivirus, antispam and firewall capabilities. This section explains how to configure dialup VPN connections between a FortiGate unit and one or more FortiClient Endpoint Security applications.

FortiClient users are usually mobile or remote users who need to connect to a private network behind a FortiGate unit. For example, the users might be employees who connect to the office network while traveling or from their homes.

For greatest ease of use, the FortiClient application can download the VPN settings from the FortiGate unit to configure itself automatically. This section covers both automatic and manual configuration.

The following topics are included in this section:

Configuration overview
FortiClient-to-FortiGate VPN configuration steps
Configure the FortiGate unit
Configure the FortiClient Endpoint Security application
Adding XAuth authentication
FortiClient dialup-client configuration example

Configuration overview

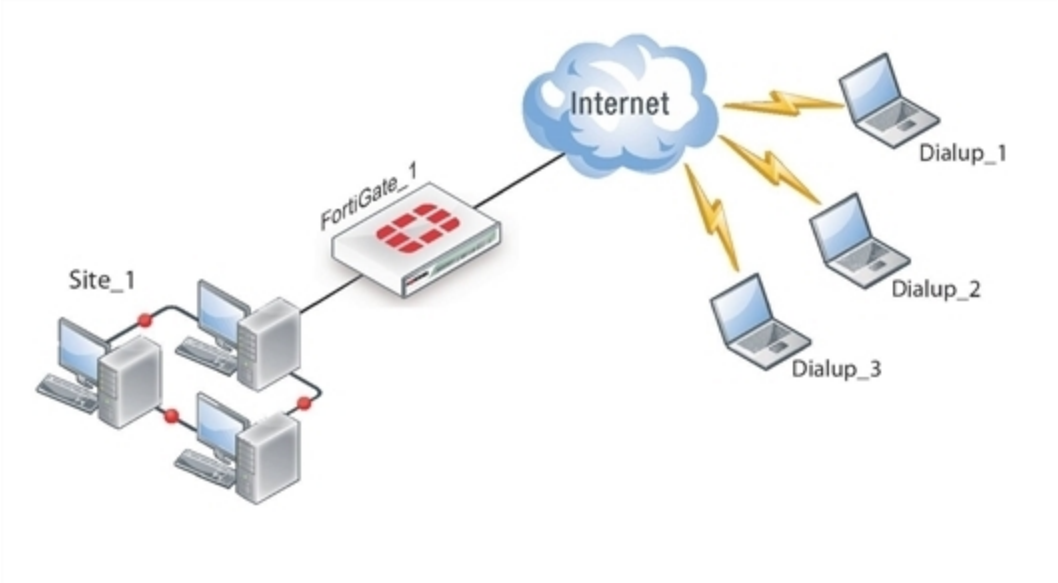
Dialup users typically obtain dynamic IP addresses from an ISP through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE). Then, the FortiClient Endpoint Security application initiates a connection to a FortiGate dialup server.

By default the FortiClient dialup client has the same IP address as the host PC on which it runs. If the host connects directly to the Internet, this is a public IP address. If the host is behind a NAT device, such as a router, the IP address is a private IP address. The NAT device must be NAT traversal (NAT-T) compatible to pass encrypted packets (see Phase 1 parameters on page 1581). The FortiClient application also can be configured to use a virtual IP address (VIP). For the duration of the connection, the FortiClient application and the FortiGate unit both use the VIP address as the IP address of the FortiClient dialup client.

For a faster and easier method of configuring a FortiGate-to-FortiClient VPN, see One button FortiGate-to-FortiClient Phase 1 VPN on page 1656.

The FortiClient application sends its encrypted packets to the VPN remote gateway, which is usually the public interface of the FortiGate unit. It also uses this interface to download VPN settings from the FortiGate unit. See Automatic configuration of FortiClient dialup clients on page 1655.

Example FortiClient dialup-client configuration



Peer identification

The FortiClient application can establish an IPsec tunnel with a FortiGate unit configured to act as a dialup server. When the FortiGate unit acts as a dialup server, it does not identify the client using the Phase 1 remote gateway address. The IPsec tunnel is established if authentication is successful and the IPsec security policy associated with the tunnel permits access. If configured, the FortiGate unit could also require FortiClient registration, that is, the remote user would be required to have FortiClient installed before connection is completed.

There are several different ways to authenticate dialup clients and restrict access to private networks based on client credentials. For more information, see Phase 1 parameters on page 1581.

Automatic configuration of FortiClient dialup clients

The FortiClient application can obtain its VPN settings from the FortiGate VPN server. FortiClient users need to know only the FortiGate VPN server IP address and their user name and password on the FortiGate unit.

The FortiGate unit listens for VPN policy requests from clients on TCP port 8900. When the dialup client connects:

- The client initiates a Secure Sockets Layer (SSL) connection to the FortiGate unit.
- The FortiGate unit requests a user name and password from the FortiClient user. Using these credentials, it authenticates the client and determines which VPN policy applies to the client.
- Provided that authentication is successful, the FortiGate unit downloads a VPN policy to the client over the SSL connection. The information includes IPsec Phase 1 and Phase 2 settings, and the IP addresses of the private networks that the client is authorized to access.
- The client uses the VPN policy settings to establish an IPsec Phase 1 connection and Phase 2 tunnel with the FortiGate unit.

One button FortiGate-to-FortiClient Phase 1 VPN

On the FortiOS VPN IKE page there is a method to create a Phase 1 portion of a VPN tunnel between the FortiGate and FortiClient. Very little information is required for this configuration. No encryption or authentication method is required. This feature is ideal for setting up quick VPN connections with basic settings.

On the Phase 1 screen is the option **Create a FortiClient VPN.** When selected, the FortiGate uint requires a few basic VPN configuration related questions. Once all the information is added, select **OK**. This will create a new dial-up IPsec-interface mode tunnel. Phase 1 and Phase 2 will be added using the default IKE settings.

The following Settings will be used when creating a one-button FortiClient VPN Phase 1 object:

- Remote Gateway: Dialup User
- Mode: Aggressive
- Default setting for Phase 1 and 2 Proposals
- XAUTH Enable as Server (Auto)
- IKE mode-config will be enabled
- Peer Option set to “Any peer ID”
- Rest of the setting use the current defaults (Default value needs to be the same on FCT side)

Once the completed, you need tocreate a default Phase 2 configuration. This only requires a name for the Phase 2 object, and select the FortiClient connection Phase 1 name.

How the FortiGate unit determines which settings to apply

The FortiGate unit follows these steps to determine the configuration information to send to the FortiClient application:

1. Check the virtual domain associated with the connection to determine which VPN policies might apply.
2. Select the VPN policy that matches the dialup client’s user group and determine which tunnel (Phase 1 configuration) is involved.
3. Check all IPsec security policies that use the specified tunnel to determine which private networks the dialup clients may access.
4. Retrieve the rest of the VPN policy information from the existing IPsec Phase 1 and Phase 2 parameters in the dialup-client configuration.

Using virtual IP addresses

When the FortiClient host PC is located behind a NAT device, unintended IP address overlap issues may arise between the private networks at the two ends of the tunnel. For example, the client’s host might receive a private IP address from a DHCP server on its network that by co-incidence is the same as a private IP address on the network behind the FortiGate unit. A conflict will occur in the host’s routing table and the FortiClient Endpoint Security application will be unable to send traffic through the tunnel. Configuring virtual IP (VIP) addresses for FortiClient applications prevents this problem.

Using VIPs ensures that client IP addresses are in a predictable range. You can then define security policies that allow access only to that source address range. If you do not use VIPs, the security policies must allow all source addresses because you cannot predict the IP address for a remote mobile user.

The FortiClient application must not have the same IP address as any host on the private network behind the FortiGate unit or any other connected FortiClient application. You can ensure this by reserving a range of IP

addresses on the private network for FortiClient users. Or, you can assign FortiClient VIPs from an uncommonly used subnet such as 10.254.254.0/24 or 192.168.254.0/24.

You can reserve a VIP address for a particular client according to its device MAC address and type of connection. The DHCP server then always assigns the reserved VIP address to the client. For more information about this feature, see the “dhcp reserved-address” section in the “system” chapter of the FortiGate CLI Reference.

On the host computer, you can find out the VIP address that the FortiClient Endpoint Security application is using. For example, in Windows command prompt, type `ipconfig /all`

On Linux or Mac OS X, type `ifconfig` in a terminal window. The output will also show the IP address that has been assigned to the host Network Interface Card (NIC).

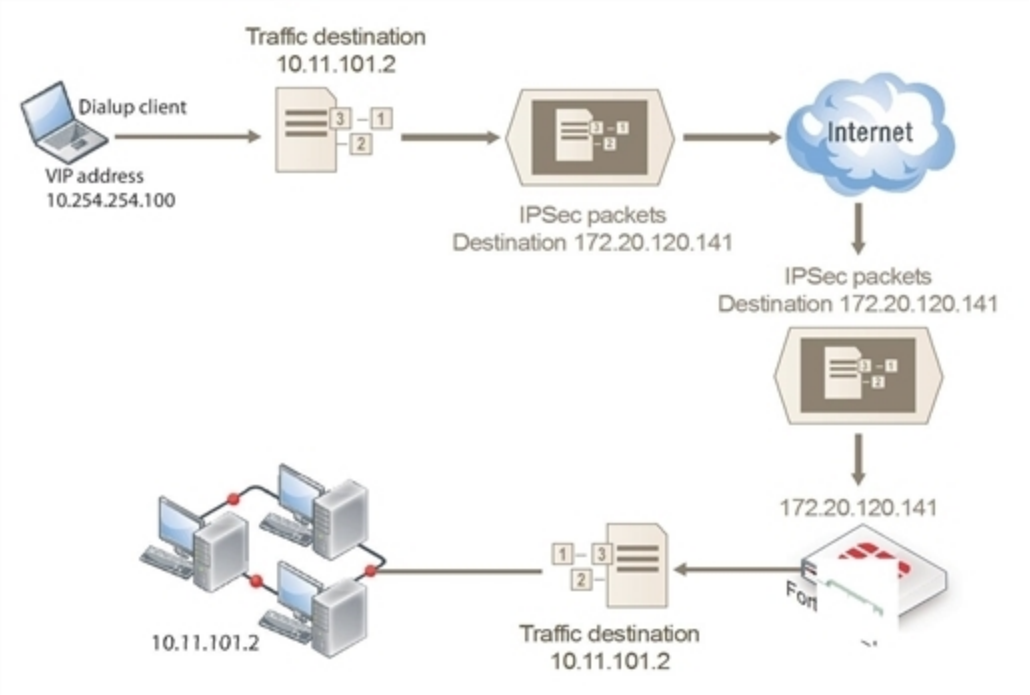
It is best to assign VIPs using DHCP over IPsec. The FortiGate dialup server can act as a DHCP server or relay requests to an external DHCP server. You can also configure VIPs manually on FortiClient applications, but it is more difficult to ensure that all clients use unique addresses.

If you assign a VIP on the private network behind the FortiGate unit and enable DHCP-IPsec (a Phase 2 advanced option), the FortiGate unit acts as a proxy on the local private network for the FortiClient dialup client. Whenever a host on the network behind the dialup server issues an ARP request for the device MAC address of the FortiClient host, the FortiGate unit answers the ARP request on behalf of the FortiClient host and forwards the associated traffic to the FortiClient host through the tunnel. For more information, see Phase 2 parameters on page 1598.

FortiGate units fully support RFC 3456. The FortiGate DHCP over IPsec feature can be enabled to allocate VIP addresses to FortiClient dialup clients using a FortiGate DHCP server.

The figure below shows an example of a FortiClient-to-FortiGate VPN where the FortiClient application is assigned a VIP on an uncommonly used subnet. The diagram also shows that while the destination for the information in the encrypted packets is the private network behind the FortiGate unit, the destination of the IPsec packets themselves is the public interface of the FortiGate unit that acts as the end of the VPN tunnel.

IP address assignments in a FortiClient dialup-client configuration



Assigning VIPs by RADIUS user group

If you use XAuth authentication, you can assign users the virtual IP address stored in the Framed-IP-Address field of their record on the RADIUS server. (See RFC 2865 and RFC 2866 for more information about RADIUS fields.) To do this:

- Set the DHCP server **IP Assignment Mode** to **User-group defined method**. This is an Advanced setting. See Configuration overview on page 1654.
- Create a new firewall user group and add the RADIUS server to it.
- In your Phase 1 settings, configure the FortiGate unit as an XAuth server and select from **User Group** the new user group that you created. For more information, see Phase 1 parameters on page 1581.
- Configure the FortiClient application to use XAuth. See Configuration overview on page 1654.

FortiClient dialup-client infrastructure requirements

- To support policy-based VPNs, the FortiGate dialup server may operate in either NAT mode or transparent mode. NAT mode is required if you want to create a route-based VPN.
- If the FortiClient dialup clients will be configured to obtain VIP addresses through FortiGate DHCP relay, a DHCP server must be available on the network behind the FortiGate unit and the DHCP server must have a direct route to the FortiGate unit.
- If the FortiGate interface to the private network is not the default gateway, the private network behind the FortiGate unit must be configured to route IP traffic destined for dialup clients back (through an appropriate gateway) to the FortiGate interface to the private network. As an alternative, you can configure the IPsec security policy on the FortiGate unit to perform inbound NAT on IP packets. Inbound NAT translates the source addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.

FortiClient-to-FortiGate VPN configuration steps

Configuring dialup client capability for FortiClient dialup clients involves the following general configuration steps:

1. If you will be using VIP addresses to identify dialup clients, determine which VIP addresses to use. As a precaution, consider using VIP addresses that are not commonly used.
2. Configure the FortiGate unit to act as a dialup server. See FortiClient-to-FortiGate VPN configuration steps on page 1659.
3. If the dialup clients will be configured to obtain VIP addresses through DHCP over IPsec, configure the FortiGate unit to act as a DHCP server or to relay DHCP requests to an external DHCP server.
4. Configure the dialup clients. See FortiClient-to-FortiGate VPN configuration steps on page 1659.

When a FortiGate unit has been configured to accept connections from FortiClient dialup-clients, you can optionally arrange to have an IPsec VPN configuration downloaded to FortiClient dialup clients automatically. For more information, see FortiClient-to-FortiGate VPN configuration steps on page 1659.

Configure the FortiGate unit

Configuring the FortiGate unit to establish VPN connections with FortiClient Endpoint Security users involves the following steps:

- Configure the VPN settings
- If the dialup clients use automatic configuration, configure the FortiGate unit as a VPN policy server
- If the dialup clients obtain VIP addresses by DHCP over IPsec, configure an IPsec DHCP server or relay

The procedures in this section cover basic setup of policy-based and route-based VPNs compatible with FortiClient Endpoint Security. A route-based VPN is simpler to configure.

Configuring FortiGate unit VPN settings

To configure FortiGate unit VPN settings to support FortiClient users, you need to:

- Configure the FortiGate Phase 1 VPN settings
- Configure the FortiGate Phase 2 VPN settings
- Add the security policy

1. On the local FortiGate unit, define the Phase 1 configuration needed to establish a secure connection with the FortiClient peer. See Phase 1 parameters on page 1581. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in Phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select **Dialup User**.
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	Select **Main (ID Protection)**.

Authentication Method	Select **Pre-shared Key**.
Pre-shared Key	Enter the pre-shared key. This must be the same preshared key provided to the FortiClient users.
Peer option	Select **Any peer ID**.

2. Define the Phase 2 parameters needed to create a VPN tunnel with the FortiClient peer. See Phase 2 parameters on page 1598. Enter these settings in particular:

Name	Enter a name to identify this Phase 2 configuration.
Phase 1	Select the name of the Phase 1 configuration that you defined.
Advanced	Select to configure the following optional setting.
DHCP-IPsec	Select if you provide virtual IP addresses to clients using DHCP.

3. Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the security policies that permit communication between the networks. For more information, see Defining VPN security policies on page 1603.

   Enter these settings in particular:
   - Define an address name for the individual address or the subnet address that the dialup users access through the VPN.
   - If FortiClient users are assigned VIP addresses, define an address name for the subnet to which these VIPs belong.
4. Define security policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see Defining VPN security policies on page 1603.

If the security policy, which grants the VPN Connection is limited to certain services, DHCP must be included, otherwise the client won't be able to retrieve a lease from the FortiGate's (IPsec) DHCP server, because the DHCP Request (coming out of the tunnel) will be blocked.

Route-based VPN security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured in Step "Configure the FortiGate unit" on page 1659.
Source Address	Select **All**.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.

Destination Address	Select **All**.
Action	Select **ACCEPT**.
Enable NAT	Disable.

If you want to allow hosts on the private network to initiate communications with the FortiClient users after the tunnel is established, you need to define a security policy for communication in that direction.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select **All**.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select **All**.
Action	Select **ACCEPT**.
Enable NAT	Disable.

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select the address name that you defined in Step "Configure the FortiGate unit" on page 1659 for the private network behind this FortiGate unit.
Outgoing Interface	Select the FortiGate unit's public interface.
Destination Address	If FortiClient users are assigned VIPs, select the address name that you defined for the VIP subnet. Otherwise, select **All**.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration that you created in Step "Configure the FortiGate unit" on page 1659. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

Place VPN policies in the policy list above any other policies having similar source and destination addresses.

Configuring the FortiGate unit as a VPN policy server

When a FortiClient application set to automatic configuration connects to the FortiGate unit, the FortiGate unit requests a user name and password. If the user supplies valid credentials, the FortiGate unit downloads the VPN settings to the FortiClient application.

You must do the following to configure the FortiGate unit to work as a VPN policy server for FortiClient automatic configuration:

1. Create user accounts for FortiClient users.
2. Create a user group for FortiClient users and the user accounts that you created in step 1.
3. Connect to the FortiGate unit CLI and configure VPN policy distribution as follows:

```
config vpn ipsec forticlient
   edit <policy_name>
      set phase2name <tunnel_name>
      set usergroupname <group_name>
      set status enable
   end
```

`<tunnel_name>` must be the Name you specified in the step 2 of Configure the FortiGate unit on page 1659. `<group_name>` must be the name of the user group your created for FortiClient users.

Configuring DHCP services on a FortiGate interface

If the FortiClient dialup clients are configured to obtain a VIP address using DHCP, configure the FortiGate dialup server to either:

- Relay DHCP requests to a DHCP server behind the FortiGate unit (see To configure DHCP relay on a FortiGate interface on page 1662 below).
- Act as a DHCP server (see To configure a DHCP server on a FortiGate interface on page 1662).

Note that DHCP services are typically configured during the interface creation stage, but you can return to an interface to modify DHCP settings if need be.

To configure DHCP relay on a FortiGate interface

1. Go to **System > Network > Interfaces** and select the interface that you want to relay DHCP.
2. Under **DHCP Server**, select **Enable** and create a new DHCP **Address Range** and **Netmask**.
3. Open the **Advanced...** menu and select **Relay** for the **Mode** option.
4. For the **Type**, select **IPsec**.
5. Select **OK**.

To configure a DHCP server on a FortiGate interface

1. Go to **System > Network > Interfaces** and select the interface that you want to act as a DHCP server.
2. Under **DHCP Server**, select **Enable** and create a new DHCP **Address Range** and **Netmask**.
3. For **Default Gateway**, enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
4. For **DNS Server**, select **Same as System DNS**. If you want to use a different DNS server for VPN clients, select ***Specify*** and enter an IP address in the available field.
5. Open the **Advanced...** menu and select **Server** for the **Mode** option.
6. For the **Type**, select **IPsec**.
7. Select **OK**.

Configure the FortiClient Endpoint Security application

The following procedure explains how to configure the FortiClient Endpoint Security application to communicate with a remote FortiGate dialup server using the VIP address that you specify manually. These procedures are based on FortiClient 5.0.

Configuring FortiClient

This procedure explains how to configure the FortiClient application manually using the default IKE and IPsec settings. For more information, refer to the FortiClient Administration Guide.

This procedure includes instructions for configuring a virtual IP for the FortiClient application, either manually or using DHCP over IPsec.

To create a FortiClient VPN configuration

1. Go to **Remote Access** and select the down-arrow for the VPN connection.
2. Select **Add new connection** and complete following information:

VPN Type	Select **IPsec VPN**.
Connection Name	Enter a descriptive name for the connection.
Remote Gateway	Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.
Authentication Method	Select **Pre-shared Key**.
Pre-shared Key	Enter the pre-shared key.
User Name	Enter the user name to connect to the tunnel.

3. Select **OK**.

Adding XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit challenges the user for a user name and password. It then forwards the user's credentials to an external RADIUS or LDAP server for verification.

Implementation of XAuth requires configuration at both the FortiGate unit and the FortiClient application. For information about configuring a FortiGate unit as an XAuth server, see Phase 1 parameters on page 1581. The following procedure explains how to configure the FortiClient application.

Note that XAuth is not compatible with IKE version 2.

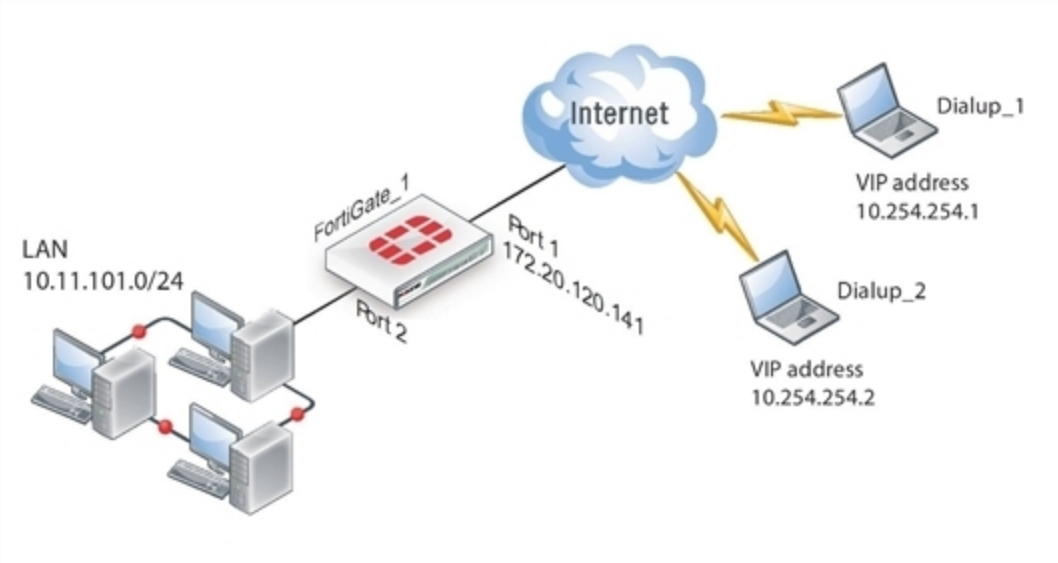
For more information on configuring XAuth authentication, see the FortiClient Administration Guide.

FortiClient dialup-client configuration example

This example demonstrates how to set up a FortiClient dialup-client IPsec VPN that uses preshared keys for authentication purposes. In the example configuration, the DHCP over IPsec feature is enabled in the FortiClient

Endpoint Security application so that the FortiClient Endpoint Security application can acquire a VIP address through the FortiGate DHCP server. Both route-based and policy-based solutions are covered.

Example FortiClient dialup-client configuration



In the example configuration:

- VIP addresses that are not commonly used (in this case, 10.254.254.0/24) are assigned to the FortiClient dialup clients using a DHCP server.
- The dialup clients are have access to the LAN behind FortiGate_1.
- The other network devices are assigned IP addresses as shown above.

Configuring FortiGate_1

When a FortiGate unit receives a connection request from a dialup client, it uses IPsec Phase 1 parameters to establish a secure connection and authenticate the client. Then, if the security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec Phase 2 parameters and applies the IPsec security policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed at the FortiGate unit:

- Define the Phase 1 parameters that the FortiGate unit needs to authenticate the dialup clients and establish a secure connection. See To define the Phase 1 parameters on page 1665.
- Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel and enable all dialup clients having VIP addresses on the 10.254.254.0/24 network to connect using the same tunnel definition. See To define the Phase 2 parameters on page 1665.
- Create security policy to control the permitted services and permitted direction of traffic between the IP source address and the dialup clients. See To define the firewall addresses on page 1665.
- Configure the FortiGate unit to service DHCP requests from dialup clients. See Configuring the FortiClient Endpoint Security application on page 1667.

To define the Phase 1 parameters

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**:

Name	todialups
Remote Gateway	Dialup User
Local Interface	Port 1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	hardtoguess
Peer Options	Any peer ID
Advanced	Select

To define the Phase 2 parameters

1. Open the **Phase 2 Selectors** panel.
2. Select **Advanced**, enter the following information, and select **OK**:

Name	td_2
Phase 1	todialups
Advanced	DHCP-IPsec

To define the firewall addresses

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New**, enter the following information, and select **OK**:

Name	internal_net
Type	Subnet
Subnet/IP Range	10.11.101.0/24
Interface	Port 2

3. Select **Create New**, enter the following information, and select **OK**:

Name	dialups
Type	IP Range

Subnet/IP Range	10.254.254.1-10.254.254.10
Interface	Route-based VPN: todialups Policy-based VPN: Any

The security policies for route-based and policy-based VPNs are described in separate sections below.

To define security policies - route-based VPN

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information, and select **OK**:

Incoming Interface	todialups
Source Address	dialups
Outgoing Interface	Port 2
Destination Address	internal_net
Action	ACCEPT
Enable NAT	Disable

4. Select **Create New**.
5. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
6. Enter the following information, and select **OK**:

Incoming Interface	Port 2
Source Address	internal_net
Outgoing Interface	todialups
Destination Address	dialups
Action	ACCEPT
Enable NAT	Disable

7. Select **Create New**.
8. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
9. Enter the following information, and select **OK**:

Incoming Interface	Port 2
Source Address	internal_net

Outgoing Interface	todialups
Destination Address	all
Service	DHCP
Action	ACCEPT
Enable NAT	Disable

10. Place these policies in the policy list above any other policies having similar source and destination addresses.

The policy in step "FortiClient dialup-client configuration example" on page 1663 is required for DHCP to function properly for policy-based VPNs. You can omit this policy if you change the **Destination Address Name** to `all` in the step before. Route-based policies are not affected by this.

To define the security policy - policy-based VPN

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	Port 2
Source Address	internal_net
Outgoing Interface	Port 1
Destination Address	dialups
VPN Tunnel	Select **Use Existing** and select **todialups** from the drop-down list.
Allow traffic to be initiated from the remote site	Enable

3. Place the policy in the policy list above any other policies having similar source and destination addresses.

Configuring the FortiClient Endpoint Security application

The following procedure explains how to configure the FortiClient Endpoint Security application to connect to FortiGate_1 and broadcast a DHCP request. The dialup client uses the VIP address acquired through FortiGate DHCP relay as its IP source address for the duration of the connection.

To configure FortiClient

1. Go to **Remote Access** and select the down-arrow for the VPN connection.
2. Select **Add new connection** and complete following information:

VPN Type	Select **IPsec VPN**.
Connection Name	Headquarters.
Remote Gateway	The port1 IP address.

Authentication Method	Select **Pre-shared Key**.
Pre-shared Key	hardtoguess
User Name	Enter the user name to connect to the tunnel.

3. Select **OK**.

FortiGate dialup-client configurations

This section explains how to set up a FortiGate dialup-client IPsec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit having a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

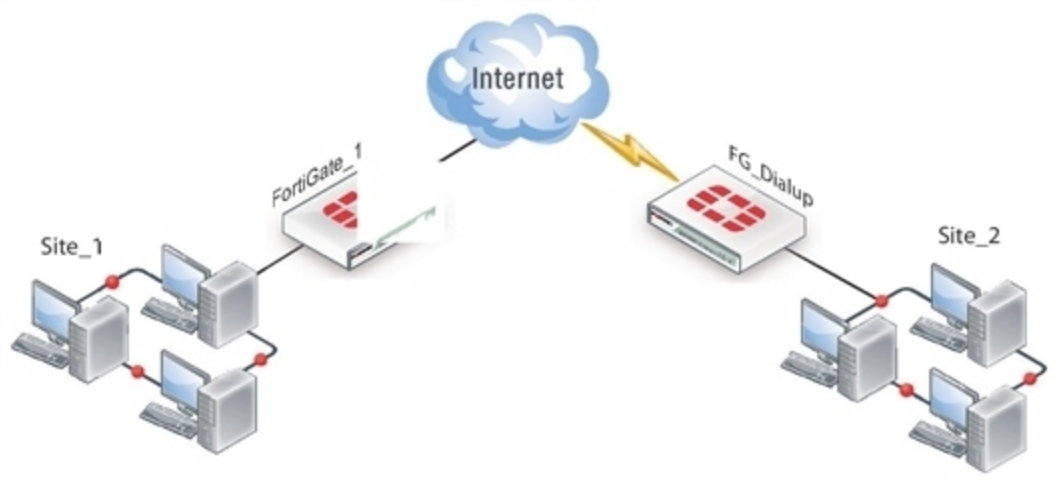
The following topics are included in this section:

Configuration overview
FortiGate dialup-client configuration steps
Configure the server to accept FortiGate dialup-client connections
Configure the FortiGate dialup client

Configuration overview

A dialup client can be a FortiGate unit. The FortiGate dialup client typically obtains a dynamic IP address from an ISP through the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) before initiating a connection to a FortiGate dialup server.

Example FortiGate dialup-client configuration



In a dialup-client configuration, the FortiGate dialup server does not rely on a Phase 1 remote gateway address to establish an IPsec VPN connection with dialup clients. As long as authentication is successful and the IPsec security policy associated with the tunnel permits access, the tunnel is established.

Several different ways to authenticate dialup clients and restrict access to private networks based on client credentials are available. To authenticate FortiGate dialup clients and help to distinguish them from FortiClient dialup clients when multiple clients will be connecting to the VPN through the same tunnel, best practices dictate that you assign a unique identifier (local ID or peer ID) to each FortiGate dialup client. For more information, see Phase 1 parameters on page 1581.

Whenever you add a unique identifier (local ID) to a FortiGate dialup client for identification purposes, you must select Aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server. For more information, see Phase 1 parameters on page 1581.

Users behind the FortiGate dialup server cannot initiate the tunnel because the FortiGate dialup client does not have a static IP address. After the tunnel is initiated by users behind the FortiGate dialup client, traffic from the private network behind the FortiGate dialup server can be sent to the private network behind the FortiGate dialup client.

Encrypted packets from the FortiGate dialup client are addressed to the public interface of the dialup server. Encrypted packets from the dialup server are addressed either to the public IP address of the FortiGate dialup client (if the dialup client connects to the Internet directly), or if the FortiGate dialup client is behind a NAT device, encrypted packets from the dialup server are addressed to the public IP address of the NAT device.

If a router with NAT capabilities is in front of the FortiGate dialup client, the router must be NAT-T compatible for encrypted traffic to pass through the NAT device. For more information, see Phase 1 parameters on page 1581.

When the FortiGate dialup server decrypts a packet from the FortiGate dialup client, the source address in the IP header may be one of the following values, depending on the configuration of the network at the far end of the tunnel:

- If the FortiGate dialup client connects to the Internet directly, the source address will be the private IP address of a host or server on the network behind the FortiGate dialup client.
- If the FortiGate dialup client is behind a NAT device, the source address will be the public IP address of the NAT device.

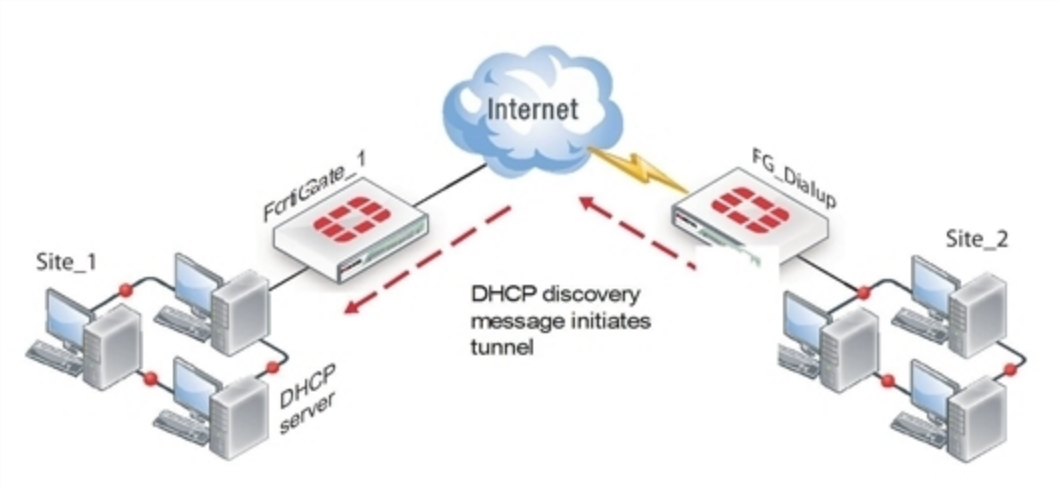
In some cases, computers on the private network behind the FortiGate dialup client may (by co-incidence) have IP addresses that are already used by computers on the network behind the FortiGate dialup server. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and traffic destined for the remote network through the tunnel may not be sent.

In many cases, computers on the private network behind the FortiGate dialup client will most likely obtain IP addresses from a local DHCP server behind the FortiGate dialup client. However, unless the local and remote networks use different private network address spaces, unintended ambiguous routing and IP-address overlap issues may arise.

To avoid these issues, you can configure FortiGate DHCP relay on the dialup client instead of using a DHCP server on the network behind the dialup client. The FortiGate dialup client can be configured to relay DHCP requests from the local private network to a DHCP server that resides on the network behind the FortiGate dialup server. You configure the FortiGate dialup client to pass traffic from the local private network to the remote network by enabling FortiGate DHCP relay on the FortiGate dialup client interface that is connected to the local private network.

Afterward, when a computer on the network behind the dialup client broadcasts a DHCP request, the dialup client relays the message through the tunnel to the remote DHCP server. The remote DHCP server responds with a private IP address for the computer. To avoid ambiguous routing and network overlap issues, the IP addresses assigned to computers behind the dialup client cannot match the network address space used by the private network behind the FortiGate dialup server.

Preventing network overlap in a FortiGate dialup-client configuration



When the DHCP server resides on the private network behind the FortiGate dialup server, the IP destination address specified in the IPsec security policy on the FortiGate dialup client must refer to that network.

You must add a static route to the DHCP server FortiGate unit if it is not directly connected to the private network behind the FortiGate dialup server; its IP address does not match the IP address of the private network. Also, the destination address in the IPsec security policy on the FortiGate dialup client must refer to the DHCP server address. The DHCP server must be configured to assign a range of IP addresses different from the DHCP server's local network, and also different from the private network addresses behind the FortiGate dialup server. See Dynamic DNS configuration on page 1639.

FortiGate dialup-client infrastructure requirements

The requirements are:

- The FortiGate dialup server must have a static public IP address.
- NAT mode is required if you want to create a route-based VPN.
- The FortiGate dialup server may operate in either NAT mode or transparent mode to support a policy-based VPN.
- Computers on the private network behind the FortiGate dialup client can obtain IP addresses either from a DHCP server behind the FortiGate dialup client, or a DHCP server behind the FortiGate dialup server.
  - If the DHCP server resides on the network behind the dialup client, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup server.
  - If the DHCP server resides on the network behind the FortiGate dialup server, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup client.

FortiGate dialup-client configuration steps

The procedures in this section assume that computers on the private network behind the FortiGate dialup client obtain IP addresses from a local DHCP server. The assigned IP addresses do not match the private network behind the FortiGate dialup server.

In situations where IP-address overlap between the local and remote private networks is likely to occur, FortiGate DHCP relay can be configured on the FortiGate dialup client to relay DHCP requests to a DHCP server behind the FortiGate dialup server. For more information, see FortiClient dialup-client configurations on page 1654.

Configuring dialup client capability for FortiGate dialup clients involves the following general configuration steps:

- Determine which IP addresses to assign to the private network behind the FortiGate dialup client, and add the IP addresses to the DHCP server behind the FortiGate dialup client. Refer to the software supplier's documentation to configure the DHCP server.
- Configure the FortiGate dialup server. See FortiGate dialup-client configuration steps on page 1671.
- Configure the FortiGate dialup client. See FortiGate dialup-client configuration steps on page 1671.

Configure the server to accept FortiGate dialup-client connections

Before you begin, optionally reserve a unique identifier (peer ID) for the FortiGate dialup client. The dialup client will supply this value to the FortiGate dialup server for authentication purposes during the IPsec Phase 1 exchange. In addition, the value will enable you to distinguish FortiGate dialup-client connections from FortiClient dialup-client connections. The same value must be specified on the dialup server and on the dialup client.

1. At the FortiGate dialup server, define the Phase 1 parameters needed to authenticate the FortiGate dialup client and establish a secure connection. See Phase 1 parameters on page 1581. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in Phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select **Dialup User**.
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	If you will be assigning an ID to the FortiGate dialup client, select **Aggressive**.
Peer Options	If you will be assigning an ID to the FortiGate dialup client, select **This peer ID** and type the identifier that you reserved for the FortiGate dialup client into the adjacent field.

2. Define the Phase 2 parameters needed to create a VPN tunnel with the FortiGate dialup client. See Phase 2 parameters on page 1598. Enter these settings in particular:

Name	Enter a name to identify this Phase 2 configuration.
Phase 1	Select the name of the Phase 1 configuration that you defined.

3. Define names for the addresses or address ranges of the private networks that the VPN links. See Defining VPN security policies on page 1603. Enter these settings in particular:
   - Define an address name for the server, host, or network behind the FortiGate dialup server.
   - Define an address name for the private network behind the FortiGate dialup client.

4. Define the security policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see Defining VPN security policies on page 1603.

Route-based VPN security policy

Define an ACCEPT security policy to permit communications between hosts on the private network behind the FortiGate dialup client and the private network behind this FortiGate dialup server. Because communication cannot be initiated in the opposite direction, there is only one policy.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the VPN tunnel (IPsec interface) created in Step 1.
Source Address	Select **All**.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select **All**.
Action	Select **ACCEPT**.
Enable NAT	Disable

Policy-based VPN security policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select the address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select the FortiGate unit's public interface.
Destination Address	Select the address name that you defined.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration that you created in Step1. from the drop-down list. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel. Clear **Allow outbound** to prevent traffic from the local network from initiating the tunnel after the tunnel has been established.

3. To prevent traffic from the local network from initiating the tunnel after the tunnel has been established, you need to disable the outbound VPN traffic in the CLI

```
config firewall policy
   edit <policy_number>
      set outbound disable
end
```

Place the policy in the policy list above any other policies having similar source and destination addresses.

If configuring a route-based policy, configure a default route for VPN traffic on this interface.

Configure the FortiGate dialup client

Configure the FortiGate dialup client.

1. At the FortiGate dialup client, define the Phase 1 parameters needed to authenticate the dialup server and establish a secure connection. See Phase 1 parameters on page 1581. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel.
Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the dialup server's public interface.
Local Interface	Select the interface that connects to the public network.
Mode	The FortiGate dialup client has a dynamic IP address, select **Aggressive**.
Advanced	Select to view the following options.
Local ID	If you defined a peer ID for the dialup client in the FortiGate dialup server configuration, enter the identifier of the dialup client. The value must be identical to the peer ID that you specified previously in the FortiGate dialup server configuration.

2. Define the Phase 2 parameters needed to create a VPN tunnel with the dialup server. See Phase 2 parameters on page 1598. Enter these settings in particular:

Name	Enter a name to identify this Phase 2 configuration.
Phase 1	Select the name of the Phase 1 configuration that you defined.

3. Define names for the addresses or address ranges of the private networks that the VPN links. See Defining VPN security policies on page 1603. Enter these settings in particular:
   - Define an address name for the server, host, or network behind the FortiGate dialup server.
   - Define an address name for the private network behind the FortiGate dialup client.
4. Define security policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see Defining VPN security policies on page 1603.

Route-based VPN security policy

Define an ACCEPT security policy to permit communications between hosts on the private network behind this FortiGate dialup client and the private network behind the FortiGate dialup server. Because communication cannot be initiated in the opposite direction, there is only one policy.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** of **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select **All**.
Outgoing Interface	Select the VPN tunnel (IPsec interface) created in Step 1.
Destination Address	Select **All**.
Action	Select **ACCEPT**.
Enable NAT	Disable

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select the address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select the FortiGate unit's public interface.
Destination Address	Select the address name that you defined for the private network behind the dialup server.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration that you created in Step "Configure the FortiGate dialup client " on page 1674 from the drop-down list. Clear **Allow traffic to be initiated from the remote site** to prevent traffic from the remote network from initiating the tunnel after the tunnel has been established.

Place the policy in the policy list above any other policies having similar source and destination addresses.

Supporting IKE Mode config clients

IKE Mode Config is an alternative to DHCP over IPsec. A FortiGate unit can be configured as either an IKE Mode Config server or client. This chapter contains the following sections:

Automatic configuration overview
IKE Mode Config overview
Configuring IKE Mode Config
Example FortiGate unit as IKE Mode Config server
Example FortiGate unit as IKE Mode Config client

Automatic configuration overview

VPN configuration for remote clients is simpler if it is automated. Several protocols support automatic configuration:

- The Fortinet FortiClient Endpoint Security application can completely configure a VPN connection with a suitably configured FortiGate unit given only the FortiGate unit's address. This protocol is exclusive to Fortinet. For more information, see FortiClient dialup-client configurations on page 1654.
- DHCP over IPsec can assign an IP address, Domain, DNS and WINS addresses. The user must first configure IPsec parameters such as gateway address, encryption and authentication algorithms.
- IKE Mode Config can configure host IP address, Domain, DNS and WINS addresses. The user must first configure IPsec parameters such as gateway address, encryption and authentication algorithms. Several network equipment vendors support IKE Mode Config, which is described in the ISAKMP Configuration Method document draft-dukes-ike-mode-cfg-02.txt.

This chapter describes how to configure a FortiGate unit as either an IKE Mode Config server or client.

IKE Mode Config overview

Dialup VPN clients connect to a FortiGate unit that acts as a VPN server, providing the client the necessary configuration information to establish a VPN tunnel. The configuration information typically includes a virtual IP address, netmask, and DNS server address.

IKE Mode Config is available only for VPNs that are route-based, also known as interface-based. A FortiGate unit can function as either an IKE Configuration Method server or client. IKE Mode Config is configurable only in the CLI.

Configuring IKE Mode Config

IKE Mode Config is configured with the CLI command `config vpn ipsec phase1-interface`. The `mode-cfg` variable enables IKE Mode Config. The `type` field determines whether you are creating an IKE Mode Config server or a client. Setting `type` to `dynamic` creates a server configuration, otherwise the configuration is a client.

Configuring an IKE Mode Config client

If the FortiGate unit will connect as a dialup client to a remote gateway that supports IKE Mode Config, the relevant `vpn ipsec phase1-interface` variables are as follows:

Variable	Description
`ike-version 1`	IKE v1 is the default for FortiGate IPsec VPNs. IKE Mode Config is also compatible with IKE v2 (RFC 4306). Use syntax `ike-version 2`.
`mode-cfg enable`	Enable IKE Mode Config.
`type {ddns | static}`	If you set `type` to `dynamic`, an IKE Mode Config server is created.
`assign-ip {enable | disable}`	Enable to request an IP address from the server.
`interface <interface_name>`	This is a regular IPsec VPN field. Specify the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.
`proposal <encryption_combination>`	This is a regular IPsec VPN field that determines the encryption and authentication settings that the client will accept. For more information, see Phase 1 parameters on page 1581.
`mode-cfg-ip-version {4|6}`	Select if the Method client receives an IPv4 or IPv6 IP address. The default is `4`. the `ip-version` setting matches this variable's value.
`ip-version <4 | 6>`	This is a regular IPsec VPN field. By default, IPsec VPNs use IPv4 addressing. You can set `ip-version` to `6` to create a VPN with IPv6 addressing.

For a complete list of available variables, see the CLI Reference.

Configuring an IKE Mode Config server

If the FortiGate unit will accept connection requests from dialup clients that support IKE Mode Config, the following `vpn ipsec phase1-interface` settings are required before any other configuration is attempted:

Variable	Description
`ike-version 1`	IKE v1 is the default for FortiGate IPsec VPNs. IKE Mode Config is also compatible with IKE v2 (RFC 4306). Use syntax `ike-version 2`.
`mode-cfg enable`	Enable IKE Mode Config.
`type dynamic`	Any other setting creates an IKE Mode Config client.
`interface <interface_name>`	This is a regular IPsec VPN field. Specify the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.
`proposal <encryption_combination>`	This is a regular IPsec VPN field that determines the encryption and authentication settings that the server will accept. For more information, see Phase 1 parameters on page 1581.
`ip-version <4 | 6>`	This is a regular IPsec VPN field. By default, IPsec VPNs use IPv4 addressing. You can set `ip-version` to `6` to create a VPN with IPv6 addressing.

For a complete list of available variables, see the CLI Reference.

After you have enabled the basic configuration, you can configure:

- IP address assignment for clients
- DNS and WINS server assignment

IP address assignment

Usually you will want to assign IP addresses to clients. The simplest method is to assign addresses from a specific range, similar to a DHCP server.

If your clients are authenticated by a RADIUS server, you can obtain the user's IP address assignment from the Framed-IP-Address attribute. The user must be authenticated using XAuth.

IKE Mode Config can also use a remote DHCP server to assign the client IP addresses. Up to eight addresses can be selected for either IPv4 or IPv6. After the DHCP proxy has been configured, the `assign-ip-from` command is used to assign IP addresses via DHCP.

To assign IP addresses from an address range - CLI

If your VPN uses IPv4 addresses,

```
config vpn ipsec phase1-interface
   edit vpn1
      set mode-cfg-ipversion 4
      set assign-ip enable
      set assign-ip-type ip
      set assign-ip-from range
      set ipv4-start-ip <range_start>
      set ipv4-end-ip <range_end>
      set ipv4-netmask <netmask>
```

```
   end
```

If your VPN uses IPv6 addresses,

```
config vpn ipsec phase1-interface
   edit vpn1
      set mode-cfg-ipversion 6
      set assign-ip enable
      set assign-ip-type ip
      set assign-ip-from range
      set ipv6-start-ip <range_start>
      set ipv6-end-ip <range_end>
   end
```

To assign IP addresses from a RADIUS server - CLI

The users must be authenticated by a RADIUS server and assigned to the FortiGate user group `<grpname>`. Since the IP address will not be static, `type` is set to dynamic, and `mode-cfg` is enabled. This is IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides.

```
config vpn ipsec phase1-interface
   edit vpn1
      set type dynamic
         set mode-cfg enable
         set assign-ip enable
         set assign-ip-from usrgrp
         set xauthtype auto
         set authusrgrp <grpname>
   end
```

To assign IP address from DHCP - CLI

The DHCP proxy must first be enabled for IKE Mode Config to use DHCP to assign the VPN client IP address(es).

```
config system settings
   set dhcp-proxy enable
   set dhcp-server-ip [ipv4 address]
   set dhcp6-server-ip [ipv6-address]
```

(Up to 8 server addresses can be configured)

```
end

config vpn ipsec phase1-interface
   edit vpn1
      set mode-cfg enable
      set assign-ip-from dhcp
   next
end
```

Certificate groups

IKE certificate groups consisting of up to four RSA certificates can be used in IKE Phase 1. Since CA and local certificates are global, the IKE daemon loads them once for all VDOMs and indexes them into trees based on subject and public key hash (for CA certificates), or certificate name (for local certicates). Certifcates are linked

together based on the issuer, and certificate chains are built by traversing these links. This reduces the need to keep multiple copies of certificates that could exist in multiple chains.

IKE certificate groups can be configured through the CLI.

Configuring the IKE local ID (CLI):

```
config vpn certificate local
edit <name>
   set ike-localid <string>
   set ike-localid-type {asnldn | fqdn}
end
```

Example FortiGate unit as IKE Mode Config server

In this example, the FortiGate unit assigns IKE Mode Config clients addresses in the range of 10.11.101.160 through 10.11.101.180. DNS and WINS server addresses are also provided. The public interface of the FortiGate unit is Port 1.

When IKE Mode-Configuration is enabled, multiple server IPs can be defined in IPsec Phase 1.

The `ipv4-split-include` variable specifies a firewall address that represents the networks to which the clients will have access. This destination IP address information is sent to the clients.

Only the CLI fields required for IKE Mode Config are shown here. For detailed information about these variables, see the FortiGate CLI Reference.

```
config vpn ipsec phase1-interface
edit "vpn-p1"
   set type dynamic
   set interface "wan1"
   set xauthtype auto
   set mode aggressive
   set mode-cfg enable
   set proposal 3des-sha1 aes128-sha1
   set dpd disable
   set dhgrp 2
   set xauthexpire on-rekey
   set authusrgrp "FG-Group1"
   set ipv4-start-ip 10.10.10.10
   set ipv4-end-ip 10.10.10.20
   set ipv4-dns-server1 1.1.1.1
   set ipv4-dns-server2 2.2.2.2
   set ipv4-dns-server3 3.3.3.3
   set ipv4-wins-server1 4.4.4.4
   set ipv4-wins-server2 5.5.5.5
   set domain "fgt1c-domain"
   set banner "fgt111C-banner"
   set backup-gateway "100.100.100.1" "host1.com" "host2"
   set ipv4-split-include OfficeLAN
end
```

Example FortiGate unit as IKE Mode Config client

In this example, the FortiGate unit connects to a VPN gateway with a static IP address that can be reached through Port 1. Only the port, gateway and proposal information needs to be configured. All other configuration

information will come from the IKE Mode Config server.

```
config vpn ipsec phase1-interface
   edit vpn1
      set ip-version 4
      set type static
      set remote-gw <gw_address>
      set interface port 1
      set proposal 3des-sha1 aes128-sha1
      set mode-cfg enable
      set mode-cfg-ipversion 4
      set assign-ip enable
   end
```

Internet-browsing configuration

This section explains how to support secure web browsing performed by dialup VPN clients, and/or hosts behind a remote VPN peer. Remote users can access the private network behind the local FortiGate unit and browse the Internet securely. All traffic generated remotely is subject to the security policy that controls traffic on the private network behind the local FortiGate unit.

The following topics are included in this section:

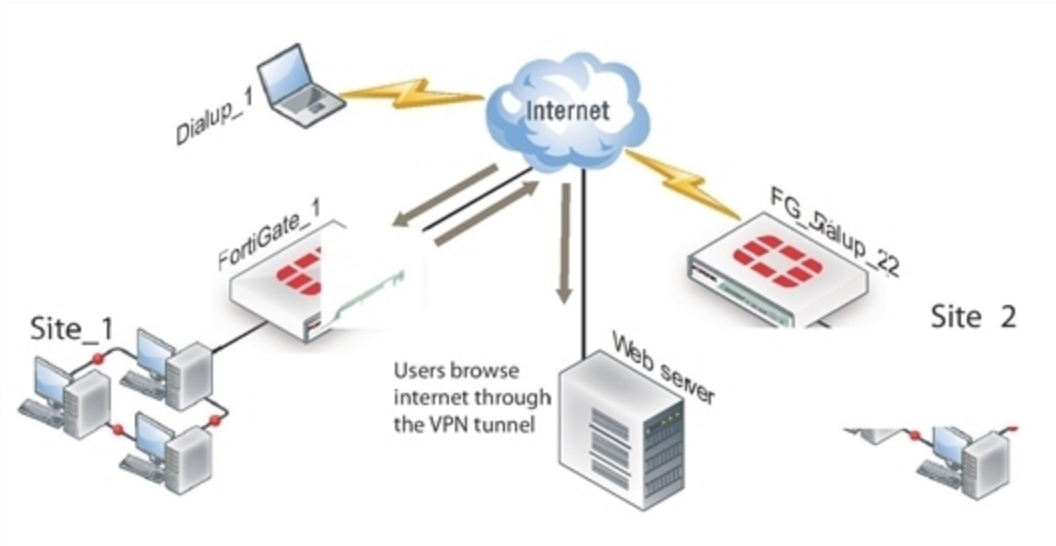
Configuration overview
Creating an Internet browsing security policy
Routing all remote traffic through the VPN tunnel

Configuration overview

A VPN provides secure access to a private network behind the FortiGate unit. You can also enable VPN clients to access the Internet securely. The FortiGate unit inspects and processes all traffic between the VPN clients and hosts on the Internet according to the Internet browsing policy. This is accomplished even though the same FortiGate interface is used for both encrypted VPN client traffic and unencrypted Internet traffic.

In the figure below, FortiGate_1 enables secure Internet browsing for FortiClient Endpoint Security users such as Dialup_1 and users on the Site_2 network behind FortiGate_2, which could be a VPN peer or a dialup client.

Example Internet-browsing configuration



You can adapt any of the following configurations to provide secure Internet browsing:

- A gateway-to-gateway configuration (see Gateway-to-gateway configurations on page 1609)
- A FortiClient dialup-client configuration (see FortiClient dialup-client configurations on page 1654)
- A FortiGate dialup-client configuration (see FortiGate dialup-client configurations on page 1669)

The procedures in this section assume that one of these configurations is in place, and that it is operating properly.

To create an internet-browsing configuration based on an existing gateway-to-gateway configuration, you must edit the gateway-to-gateway configuration as follows:

- On the FortiGate unit that will provide Internet access, create an Internet browsing security policy. See Configuration overview on page 1682, below.
- Configure the remote peer or client to route all traffic through the VPN tunnel. You can do this on a FortiGate unit or on a FortiClient Endpoint Security application. See Configuration overview on page 1682.

Creating an Internet browsing security policy

On the FortiGate unit that acts as a VPN server and will provide secure access to the Internet, you must create an Internet browsing security policy. This policy differs depending on whether your gateway-to-gateway configuration is policy-based or route-based.

To create an Internet browsing policy - policy-based VPN

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information and then select **OK**:

Incoming Interface	The interface to which the VPN tunnel is bound.
Source Address	The internal range address of the remote spoke site.
Outgoing Interface	The interface to which the VPN tunnel is bound.
Destination Address	All
VPN Tunnel	Select **Use Existing** and select the tunnel that provides access to the private network behind the FortiGate unit.
Allow traffic to be initiated from the remote site	Enable
Inbound NAT	Enable

3. Enable inbound NAT in the CLI.

```
config firewall policy
   edit <policy_number>
      set natinbound enable
end
```

To create an Internet browsing policy - route-based VPN

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information and then select **OK**:

Incoming Interface	The IPsec VPN interface.

Source Address	The internal range address of the remote spoke site.
Outgoing Interface	The interface that connects to the Internet. The virtual IPsec interface is configured on this physical interface.
Destination Address	All
Action	ACCEPT
Enable NAT	Enable

The VPN clients must be configured to route all Internet traffic through the VPN tunnel.

Routing all remote traffic through the VPN tunnel

To make use of the Internet browsing configuration on the VPN server, the VPN peer or client must route all traffic through the VPN tunnel. Usually, only the traffic destined for the private network behind the FortiGate VPN server is sent through the tunnel.

The remote end of the VPN can be a FortiGate unit that acts as a peer in a gateway-to-gateway configuration, or a FortiClient application that protects an individual client PC.

- To configure a remote peer FortiGate unit for Internet browsing via VPN, see Configuring a FortiGate remote peer to support Internet browsing on page 1684.
- To configure a FortiClient Endpoint Security application for Internet browsing via VPN, see Configuring a FortiClient application to support Internet browsing on page 1685.

These procedures assume that your VPN connection to the protected private network is working and that you have configured the FortiGate VPN server for Internet browsing as described in Routing all remote traffic through the VPN tunnel on page 1684.

Configuring a FortiGate remote peer to support Internet browsing

The configuration changes to send all traffic through the VPN differ for policy-based and route-based VPNs.

To route all traffic through a policy-based VPN

1. At the FortiGate dialup client, go to **Policy & Objects > Policy > IPv4**.
2. Select the IPsec security policy and then select **Edit**.
3. From the **Destination Address** list, select **all**.
4. Select **OK**.

Packets are routed through the VPN tunnel, not just those destined for the protected private network.

To route all traffic through a route-based VPN

1. At the FortiGate dialup client, go to **Router > Static > Static Route**s.
2. On a low-end FortiGate unit, go to **System > Network > Routing**.
3. Select the default route (destination IP 0.0.0.0) and then select ***Edit***. If there is no default route, select **Create New**. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	Select the IPsec virtual interface.
Distance	Leave at default.

All packets are routed through the VPN tunnel, not just packets destined for the protected private network.

Configuring a FortiClient application to support Internet browsing

By default, the FortiClient application configures the PC so that traffic destined for the remote protected network passes through the VPN tunnel but all other traffic is sent to the default gateway. You need to modify the FortiClient settings so that it configures the PC to route all outbound traffic through the VPN.

To route all traffic through VPN - FortiClient application

1. At the remote host, start FortiClient.
2. Go to **VPN > Connections**.
3. Select the definition that connects FortiClient to the FortiGate dialup server.
4. Select **Advanced** and then select **Edit**.
5. In the **Edit Connection** dialog box, select **Advanced**.
6. In the **Remote Network** group, select **Add**.
7. In the **IP** and **Subnet Mask** fields, type `0.0.0.0/0.0.0.0` and select **OK**.
   The address is added to the **Remote Network** list. The first destination IP address in the list establishes a VPN tunnel. The second destination address (`0.0.0.0/0.0.0.0` in this case) forces all other traffic through the VPN tunnel.
8. Select **OK**.

Redundant VPN configurations

This section discusses the options for supporting redundant and partially redundant IPsec VPNs, using route-based approaches.

The following topics are included in this section:

Configuration overview
General configuration steps
Configure the VPN peers - route-based VPN
Redundant route-based VPN configuration example
Partially-redundant route-based VPN example
Creating a backup IPsec interface

Configuration overview

A FortiGate unit with two interfaces connected to the Internet can be configured to support redundant VPNs to the same remote peer. If the primary connection fails, the FortiGate unit can establish a VPN using the other connection.

Redundant tunnels do not support Tunnel Mode or manual keys. You must use Interface Mode.

A fully-redundant configuration requires redundant connections to the Internet on both peers. The figure below shows an example of this. This is useful to create a reliable connection between two FortiGate units with static IP addresses.

When only one peer has redundant connections, the configuration is partially-redundant. For an example of this, see Configuration overview on page 1686. This is useful to provide reliable service from a FortiGate unit with static IP addresses that accepts connections from dialup IPsec VPN clients.

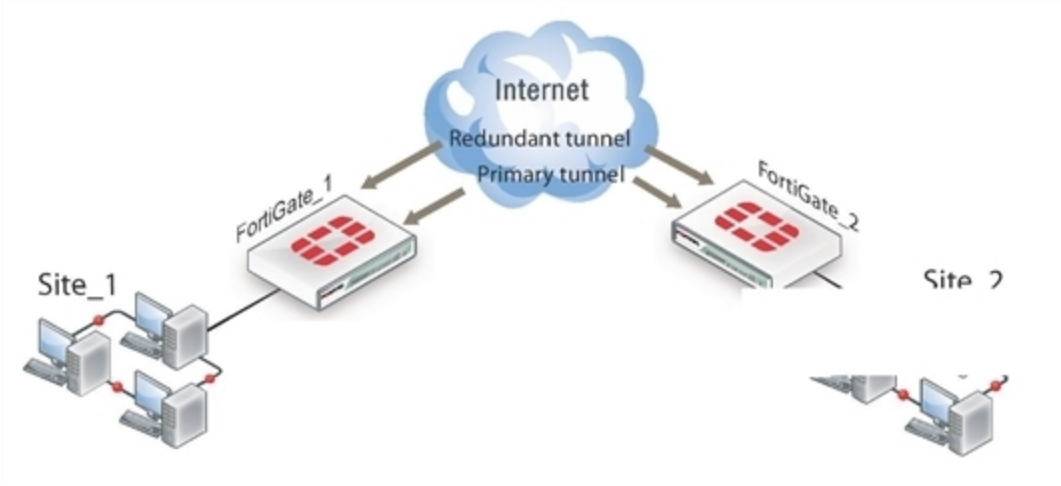
In a fully-redundant VPN configuration with two interfaces on each peer, four distinct paths are possible for VPN traffic from end to end. Each interface on a peer can communicate with both interfaces on the other peer. This ensures that a VPN will be available as long as each peer has one working connection to the Internet.

You configure a VPN and an entry in the routing table for each of the four paths. All of these VPNs are ready to carry data. You set different routing distances for each route and only the shortest distance route is used. If this route fails, the route with the next shortest distance is used.

The redundant configurations described in this chapter use route-based VPNs, otherwise known as virtual IPsec interfaces. This means that the FortiGate unit must operate in NAT mode. You must use auto-keying. A VPN that is created using manual keys cannot be included in a redundant-tunnel configuration.

The configuration described here assumes that your redundant VPNs are essentially equal in cost and capability. When the original VPN returns to service, traffic continues to use the replacement VPN until the replacement VPN fails. If your redundant VPN uses more expensive facilities, you want to use it only as a backup while the main VPN is down. For information on how to do this, see Configuration overview on page 1686.

Example redundant-tunnel configuration



A VPN that is created using manual keys cannot be included in a redundant-tunnel configuration.

General configuration steps

A redundant configuration at each VPN peer includes:

- One Phase 1 configuration (virtual IPsec interface) for each path between the two peers. In a fully-meshed redundant configuration, each network interface on one peer can communicate with each network interface on the remote peer. If both peers have two public interfaces, this means that each peer has four paths, for example.
- One Phase 2 definition for each Phase 1 configuration.
- One static route for each IPsec interface, with different distance values to prioritize the routes.
- Two Accept security policies per IPsec interface, one for each direction of traffic.
- Dead peer detection enabled in each Phase 1 definition.

The procedures in this section assume that two separate interfaces to the Internet are available on each VPN peer.

Configure the VPN peers - route-based VPN

VPN peers are configured using Interface Mode for redundant tunnels.

Configure each VPN peer as follows:

1. Ensure that the interfaces used in the VPN have static IP addresses.
2. Create a Phase 1 configuration for each of the paths between the peers.
3. Enable dead peer detection so that one of the other paths is activated if this path fails.
4. Enter these settings in particular, and any other VPN settings as required:

Path 1

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the primary interface of the remote peer.
Local Interface	Select the primary public interface of this peer.
Dead Peer Detection	Enable

Path 2

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the secondary interface of the remote peer.
Local Interface	Select the primary public interface of this peer.
Dead Peer Detection	Enable

Path 3

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the primary interface of the remote peer.
Local Interface	Select the secondary public interface of this peer.
Dead Peer Detection	Enable

Path 4

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the secondary interface of the remote peer.
Local Interface	Select the secondary public interface of this peer.
Dead Peer Detection	Enable

For more information, see Phase 1 parameters on page 1581.

5. Create a Phase 2 definition for each path. See Phase 2 parameters on page 1598. Select the Phase 1 configuration (virtual IPsec interface) that you defined for this path. You can select the name from the Static IP Address part of the list.
6. Create a route for each path to the other peer. If there are two ports on each peer, there are four possible paths between the peer devices.

Destination IP/Mask	The IP address and netmask of the private network behind the remote peer.
Device	One of the virtual IPsec interfaces on the local peer.
Distance	For each path, enter a different value to prioritize the paths.

7. Define the security policy for the local primary interface. See Defining VPN security policies on page 1603. You need to create two policies for each path to enable communication in both directions. Enter these settings in particular:

Incoming Interface	Select the local interface to the internal (private) network.
Source Address	All
Outgoing Interface	Select one of the virtual IPsec interfaces you created in Step 2.
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

8. Select **Create New**, leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**, and enter these settings:

Incoming Interface	Select one of the virtual IPsec interfaces you created in Step 2.
Source Address	All
Outgoing Interface	Select the local interface to the internal (private) network.
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

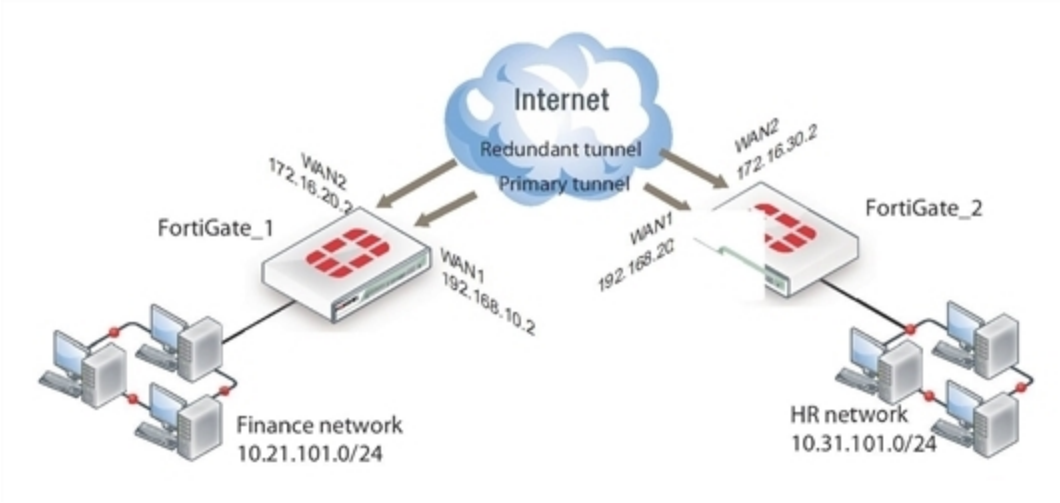
9. Place the policy in the policy list above any other policies having similar source and destination addresses.
10. Repeat this procedure at the remote FortiGate unit.

Redundant route-based VPN configuration example

This example demonstrates a fully redundant site-to-site VPN configuration using route-based VPNs. At each site, the FortiGate unit has two interfaces connected to the Internet through different ISPs. This means that there are four possible paths for communication between the two units. In this example, these paths, listed in descending priority, are:

- FortiGate_1 WAN 1 to FortiGate_2 WAN 1
- FortiGate_1 WAN 1 to FortiGate_2 WAN 2
- FortiGate_1 WAN 2 to FortiGate_2 WAN 1
- FortiGate_1 WAN 2 to FortiGate_2 WAN 2

Example redundant route-based VPN configuration



For each path, VPN configuration, security policies and routing are defined. By specifying a different routing distance for each path, the paths are prioritized. A VPN tunnel is established on each path, but only the highest priority one is used. If the highest priority path goes down, the traffic is automatically routed over the next highest priority path. You could use dynamic routing, but to keep this example simple, static routing is used.

Configuring FortiGate_1

When configuring FortiGate_1, you must:

- Configure the interfaces involved in the VPN.
- Define the Phase 1 configuration for each of the four possible paths, creating a virtual IPsec interface for each one.
- Define the Phase 2 configuration for each of the four possible paths.
- Configure routes for the four IPsec interfaces, assigning the appropriate priorities.
- Configure incoming and outgoing security policies between the internal interface and each of the virtual IPsec interfaces.

To configure the network interfaces

1. Go to **System > Network > Interfaces**.
2. Select the Internal interface and select **Edit**.

3. Enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`10.21.101.0/255.255.255.0`

4. Select the WAN1 interface and select **Edit**, enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`192.168.10.2/255.255.255.0`

5. Select the WAN2 interface and select **Edit**, enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`172.16.20.2/255.255.255.0`

To configure the IPsec interfaces (Phase 1 configurations)

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**:

Name	`Site_1_A`
Remote Gateway	Static IP Address
IP Address	`192.168.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

4. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_1_B`
Remote Gateway	Static IP Address
IP Address	`172.16.30.2`

Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

5. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_1_C`
Remote Gateway	Static IP Address
IP Address	`192.168.20.2`
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

6. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_1_D`
Remote Gateway	Static IP Address
IP Address	`172.16.30.2`
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID

Advanced	
Dead Peer Detection	Select

To define the Phase 2 configurations for the four VPNs

1. Open the **Phase 2 Selectors** panel.
2. Enter the following information and select **OK**:

Name	`Route_A`
Phase 1	Site_1_A

3. Enter the following Phase 2 information for the subsequent route:

Name	`Route_B`
Phase 1	Site_1_B

4. Enter the following Phase 2 information for the subsequent route:

Name	`Route_C`
Phase 1	Site_1_C

5. Enter the following Phase 2 information for the subsequent route:

Name	`Route_D`
Phase 1	Site_1_D

To configure routes

1. Go to **Router > Static > Static Routes**.
   For low-end FortiGate units, go to **System > Network > Routing**.
2. Select **Create New**, enter the following default gateway information and then select **OK**:

Destination IP/Mask	`0.0.0.0/0.0.0.0`
Device	WAN1
Gateway	`192.168.10.1`
Distance (Advanced)	`10`

3. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	`10.31.101.0/255.255.255.0`

Device	Site_1_A
Distance (Advanced)	1

4. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_B
Distance (Advanced)	2

5. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_C
Distance (Advanced)	3

6. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_D
Distance (Advanced)	4

To configure security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and then select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

3. Select **Create New**.
4. Enter the following information, and select **OK**:

Incoming Interface	Site_1_A
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

5. Select **Create New**.
6. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

7. Select **Create New**.
8. Enter the following information, and select **OK**:

Incoming Interface	Site_1_B
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

9. Select **Create New**.
10. Enter the following information, and select **OK**:

Incoming Interface	Internal

Source Address	All
Outgoing Interface	Site_1_C
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

11. Select **Create New**.
12. Enter the following information, and select **OK**:

Incoming Interface	Site_1_C
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

13. Select **Create New**.
14. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_D
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

15. Select **Create New**.
16. Enter the following information, and select **OK**:

Incoming Interface	Site_1_D
Source Address	All

Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

Configuring FortiGate_2

The configuration for FortiGate_2 is very similar to that of FortiGate_1. You must:

- Configure the interfaces involved in the VPN.
- Define the Phase 1 configuration for each of the four possible paths, creating a virtual IPsec interface for each one.
- Define the Phase 2 configuration for each of the four possible paths.
- Configure routes for the four IPsec interfaces, assigning the appropriate priorities.
- Configure incoming and outgoing security policies between the internal interface and each of the virtual IPsec interfaces.

To configure the network interfaces

1. Go to **System > Network > Interfaces**.
2. Select the Internal interface and then select **Edit**. Enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`10.31.101.0/255.255.255.0`

3. Select the WAN1 interface and then select **Edit**. Enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`192.168.20.2/255.255.255.0`

4. Select the WAN2 interface and then select **Edit**. Enter the following information and then select **OK**:

Addressing mode	Manual
IP/Netmask	`172.16.30.2/255.255.255.0`

To configure the IPsec interfaces (Phase 1 configurations)

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**:

Name	`Site_2_A`

Remote Gateway	Static IP Address
IP Address	`192.168.10.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

4. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_2_B`
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

5. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_2_C`
Remote Gateway	Static IP Address
IP Address	`192.168.10.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key

Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

6. Create a new tunnel and enter the following Phase 1 information:

Name	`Site_2_D`
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

To define the Phase 2 configurations for the four VPNs

1. On the first VPN route, open the **Phase 2 Selectors** panel.
2. Enter the following information and select **OK**:

Name	`Route_A`
Phase 1	`Site_2_A`

3. Enter the following Phase 2 information for the subsequent route:

Name	`Route_B`
Phase 1	`Site_2_B`

4. Enter the following Phase 2 information for the subsequent route:

Name	`Route_C`
Phase 1	`Site_2_C`

5. Enter the following Phase 2 information for the subsequent route:

Name	Route_D
Phase 1	Site_2_D

To configure routes

1. Go to **Router > Static > Static Routes**.

   For low-end FortiGate units, go to **System > Network > Routing**.
2. Select **Create New**, enter the following default gateway information and then select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	WAN1
Gateway	192.168.10.1
Distance (Advanced)	10

3. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_A
Distance (Advanced)	1

4. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_B
Distance (Advanced)	2

5. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_C
Distance (Advanced)	3

6. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_D
Distance (Advanced)	4

To configure security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

3. Select **Create New**.
4. Enter the following information, and select **OK**:

Incoming Interface	Site_2_A
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

5. Select **Create New**.
6. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

7. Select **Create New**.
8. Enter the following information, and select **OK**:

Incoming Interface	Site_2_B
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

9. Select **Create New**.
10. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_C
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

11. Select **Create New**.
12. Enter the following information, and select **OK**:

Incoming Interface	Site_2_C
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

13. Select **Create New**.
14. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_D
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

15. Select **Create New**.
16. Enter the following information, and select **OK**:

Incoming Interface	Site_2_D
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

Partially-redundant route-based VPN example

This example demonstrates how to set up a partially redundant IPsec VPN between a local FortiGate unit and a remote VPN peer that receives a dynamic IP address from an ISP before it connects to the FortiGate unit. For more information about FortiGate dialup-client configurations, see FortiGate dialup-client configurations on page 1669.

When a FortiGate unit has more than one interface to the Internet (see FortiGate_1), you can configure redundant routes. If the primary connection fails, the FortiGate unit can establish a VPN using the redundant connection.

In this case, FortiGate_2 has only one connection to the Internet. If the link to the ISP were to go down, the connection to FortiGate_1 would be lost, and the tunnel would be taken down. The tunnel is said to be partially redundant because FortiGate_2 does not support a redundant connection.

In the configuration example:

- Both FortiGate units operate in NAT mode.
- Two separate interfaces to the Internet (192.168.10.2 and 172.16.20.2) are available on FortiGate_1. Each interface has a static public IP address.
- FortiGate_2 has a single connection to the Internet and obtains a dynamic public IP address (for example, 172.16.30.1) when it connects to the Internet.

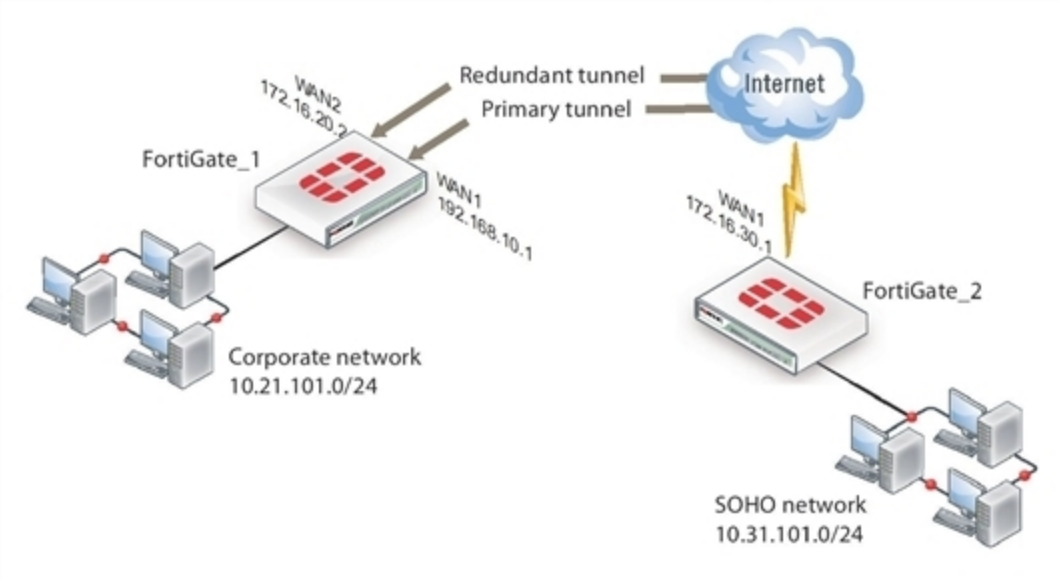
- FortiGate_2 forwards IP packets from the SOHO network (10.31.101.0/24) to the corporate network (10.21.101.0/24) behind FortiGate_1 through a partially redundant IPsec VPN. Encrypted packets from FortiGate_2 are addressed to the public interface of FortiGate_1. Encrypted packets from FortiGate_1 are addressed to the public IP address of FortiGate_2.

There are two possible paths for communication between the two units. In this example, these paths, listed in descending priority, are:

- FortiGate_1 WAN 1 to FortiGate_2 WAN 1
- FortiGate_1 WAN 2 to FortiGate_2 WAN 1

For each path, VPN configuration, security policies and routing are defined. By specifying a different routing distance for each path, the paths are prioritized. A VPN tunnel is established on each path, but only the highest priority one is used. If the highest priority path goes down, the traffic is automatically routed over the next highest priority path. You could use dynamic routing, but to keep this example simple, static routing is used.

Example partially redundant route-based configuration



Configuring FortiGate_1

Whenconfiguring FortiGate_1, you must:

- Configure the interfaces involved in the VPN.
- Define the Phase 1 configuration for each of the two possible paths, creating a virtual IPsec interface for each one.
- Define the Phase 2 configuration for each of the two possible paths.
- Configure incoming and outgoing security policies between the internal interface and each of the virtual IPsec interfaces.

To configure the network interfaces

1. Go to **System > Network > Interfaces**.
2. Select the Internal interface and select **Edit**. Enter the following information and select **OK**:

Addressing mode	Manual
IP/Netmask	10.21.101.2/255.255.255.0

3. Select the WAN1 interface and select **Edit**. Enter the following information and select **OK**:

Addressing mode	Manual
IP/Netmask	192.168.10.2/255.255.255.0

4. Select the WAN2 interface and select **Edit**. Enter the following information and select **OK**:

Addressing mode	Manual
IP/Netmask	172.16.20.2/255.255.255.0

To configure the IPsec interfaces (Phase 1 configurations)

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**:

Name	Site_1_A
Remote Gateway	Dialup User
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

4. Create a new tunnel and enter the following Phase 1 information:

Name	Site_1_B
Remote Gateway	Dialup User
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key

Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

To define the Phase 2 configurations for the two VPNs

1. Open the **Phase 2 Selectors** panel.
2. Enter the following information and select **OK**:

Name	`Route_A`
Phase 1	`Site_1_A`

3. Enter the following Phase 2 information for the subsequent route:

Name	`Route_B`
Phase 1	`Site_1_B`

To configure routes

1. Go to **Router > Static > Static Routes**.
2. For low-end FortiGate units, go to **System > Network > Routing**.
3. Select **Create New**, enter the following default gateway information and select **OK**:

Destination IP/Mask	`0.0.0.0/0.0.0.0`
Device	WAN1
Gateway	`192.168.10.1`
Distance (Advanced)	10

To configure security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_A
Destination Address	All

Schedule	Always
Service	Any
Action	ACCEPT

3. Select **Create New**.
4. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

Configuring FortiGate_2

The configuration for FortiGate_2 is similar to that of FortiGate_1. You must

- configure the interface involved in the VPN
- define the Phase 1 configuration for the primary and redundant paths, creating a virtual IPsec interface for each one
- define the Phase 2 configurations for the primary and redundant paths, defining the internal network as the source address so that FortiGate_1 can automatically configure routing
- configure the routes for the two IPsec interfaces, assigning the appropriate priorities
- configure security policies between the internal interface and each of the virtual IPsec interfaces

To configure the network interfaces

1. Go to **System > Network > Interfaces**.
2. Select the Internal interface and select **Edit**. Enter the following information and select **OK**:

Addressing mode	Manual
IP/Netmask	`10.31.101.2/255.255.255.0`

3. Select the WAN1 interface and select **Edit**. Set the **Addressing mode** to **DHCP**.

To configure the two IPsec interfaces (Phase 1 configurations)

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).
3. Enter the following information, and select **OK**:

Name	Site_2_A
Remote Gateway	Static IP Address
IP Address	192.168.10.2
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

4. Create a new tunnel and enter the following Phase 1 information:

Name	Site_2_B
Remote Gateway	Static IP Address
IP Address	172.16.20.2
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Any peer ID
Advanced	
Dead Peer Detection	Select

To define the Phase 2 configurations for the two VPNs

1. Open the **Phase 2 Selectors** panel.
2. Enter the following information and select **OK**:

Name	Route_A
Phase 1	Site_2_A
Advanced	
Source Address	10.31.101.0/24

3. Enter the following Phase 2 information for the subsequent route:

Name	`Route_B`
Phase 1	`Site_2_B`
Advanced	
Source Address	10.31.101.0/24

To configure routes

1. Go to **Router > Static > Static Routes**.

   For low-end FortiGate units, go to **System > Network > Routing**.
2. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	`10.21.101.0/255.255.255.0`
Device	Site_2_A
Distance (Advanced)	1

3. Select **Create New**, enter the following information and then select **OK**:

Destination IP/Mask	`10.21.101.0/255.255.255.0`
Device	Site_2_B
Distance (Advanced)	2

To configure security policies

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

3. Select **Create New**.
4. Enter the following information, and select **OK**:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

Creating a backup IPsec interface

You can configure a route-based VPN that acts as a backup facility to another VPN. It is used only while your main VPN is out of service. This is desirable when the redundant VPN uses a more expensive facility.

You can configure a backup IPsec interface only in the CLI. The backup feature works only on interfaces with static addresses that have dead peer detection enabled. The `monitor` option creates a backup VPN for the specified Phase 1 configuration.

In the following example, backup_vpn is a backup for main_vpn.

```
config vpn ipsec phase1-interface
   edit main_vpn
      set dpd on
      set interface port1
      set nattraversal enable
      set psksecret "hard-to-guess"
      set remote-gw 192.168.10.8
      set type static
   end
   edit backup_vpn
      set dpd on
      set interface port2
      set monitor main_vpn
      set nattraversal enable
      set psksecret "hard-to-guess"
      set remote-gw 192.168.10.8
      set type static
   end
```

Transparent mode VPNs

This section describes transparent VPN configurations, in which two FortiGate units create a VPN tunnel between two separate private networks transparently.

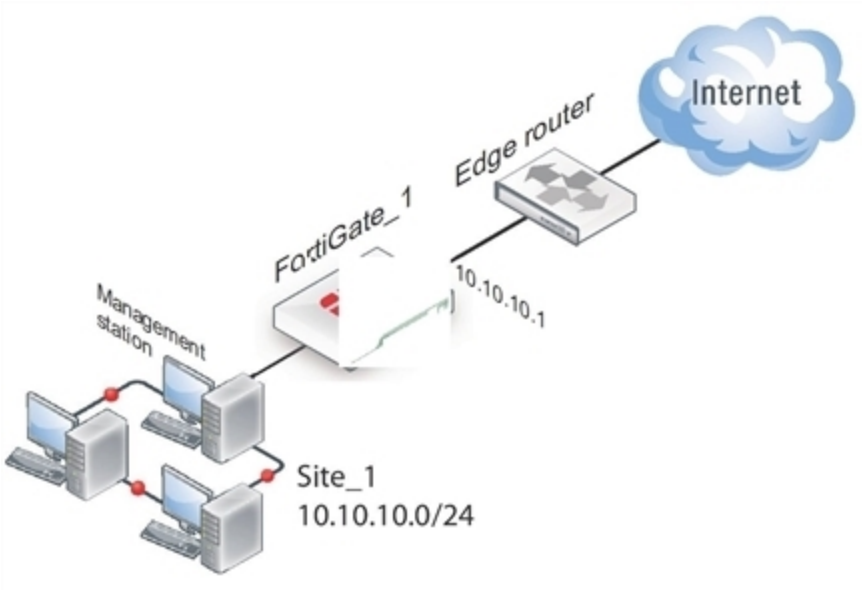
The following topics are included in this section:

Configuration overview
Configure the VPN peers

Configuration overview

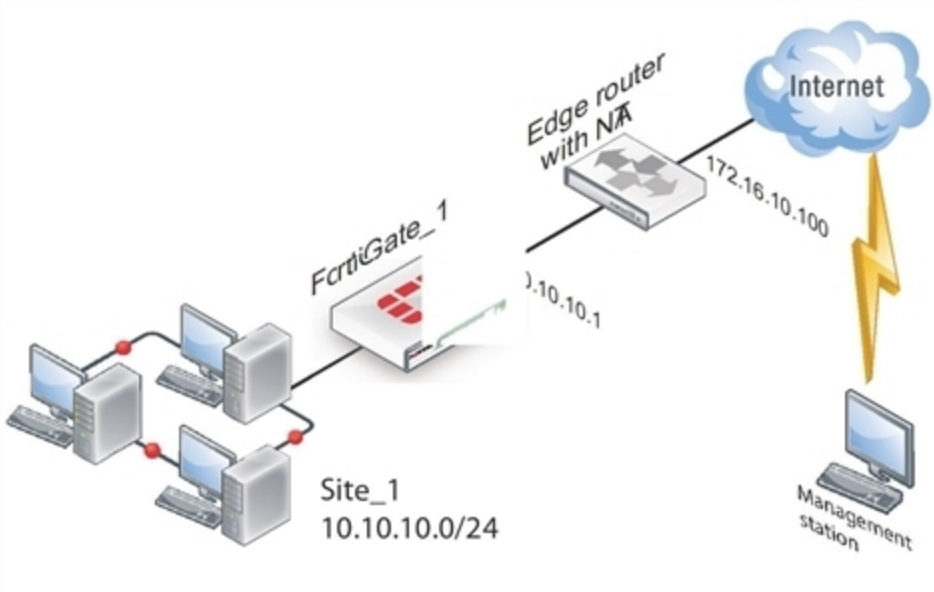
In transparent mode, all interfaces of the FortiGate unit except the management interface (which by default is assigned IP address 10.10.10.1/255.255.255.0) are invisible at the network layer. Typically, when a FortiGate unit runs in transparent mode, different network segments are connected to the FortiGate interfaces. The figure belows the management station on the same subnet. The management station can connect to the FortiGate unit directly through the web-based manager.

Management station on internal network



An edge router typically provides a public connection to the Internet and one interface of the FortiGate unit is connected to the router. If the FortiGate unit is managed from an external address (see the figure below), the router must translate (NAT) a routable address to direct management traffic to the FortiGate management interface.

Management station on external network



In a transparent VPN configuration, two FortiGate units create a VPN tunnel between two separate private networks transparently. All traffic between the two networks is encrypted and protected by FortiGate security policies.

Both FortiGate units may be running in transparent mode, or one could be running in transparent mode and the other running in NAT mode. If the remote peer is running in NAT mode, it must have a static public IP address.

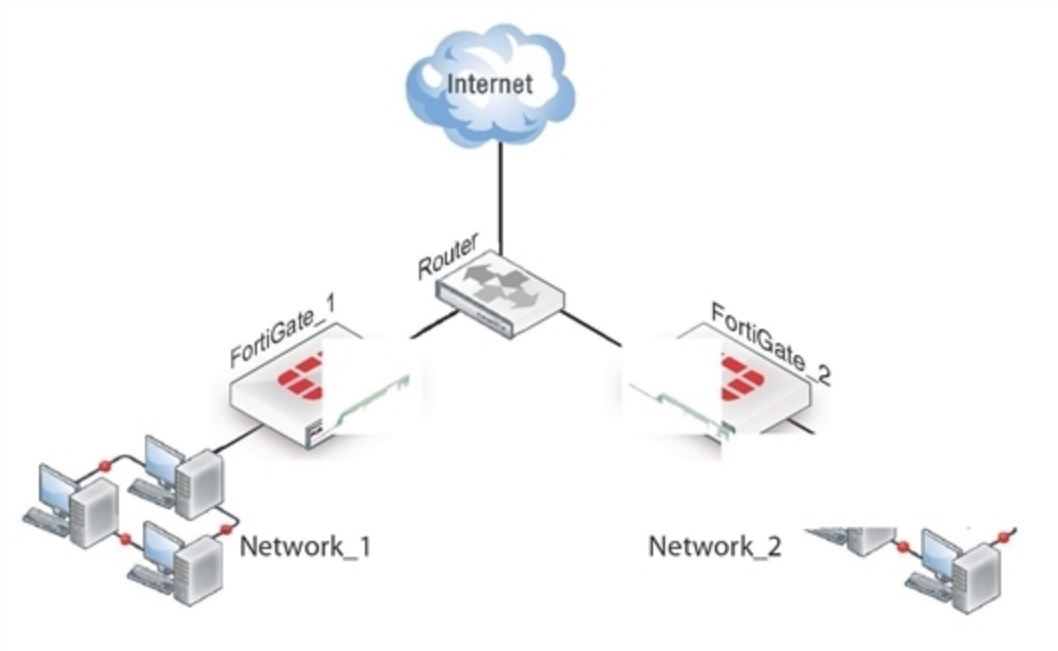
VPNs between two FortiGate units running in transparent mode do not support inbound/outbound NAT (supported through CLI commands) within the tunnel. In addition, a FortiGate unit running in transparent mode cannot be used in a hub-and-spoke configuration.

Encrypted packets from the remote VPN peer are addressed to the management interface of the local FortiGate unit. If the local FortiGate unit can reach the VPN peer locally, a static route to the VPN peer must be added to the routing table on the local FortiGate unit. If the VPN peer connects through the Internet, encrypted packets from the local FortiGate unit must be routed to the edge router instead. For information about how to add a static route to the FortiGate routing table, see the Advanced Routing Guide.

In the example configuration shown above, Network Address Translation (NAT) is enabled on the router. When an encrypted packet from the remote VPN peer arrives at the router through the Internet, the router performs inbound NAT and forwards the packet to the FortiGate unit. Refer to the software supplier's documentation to configure the router.

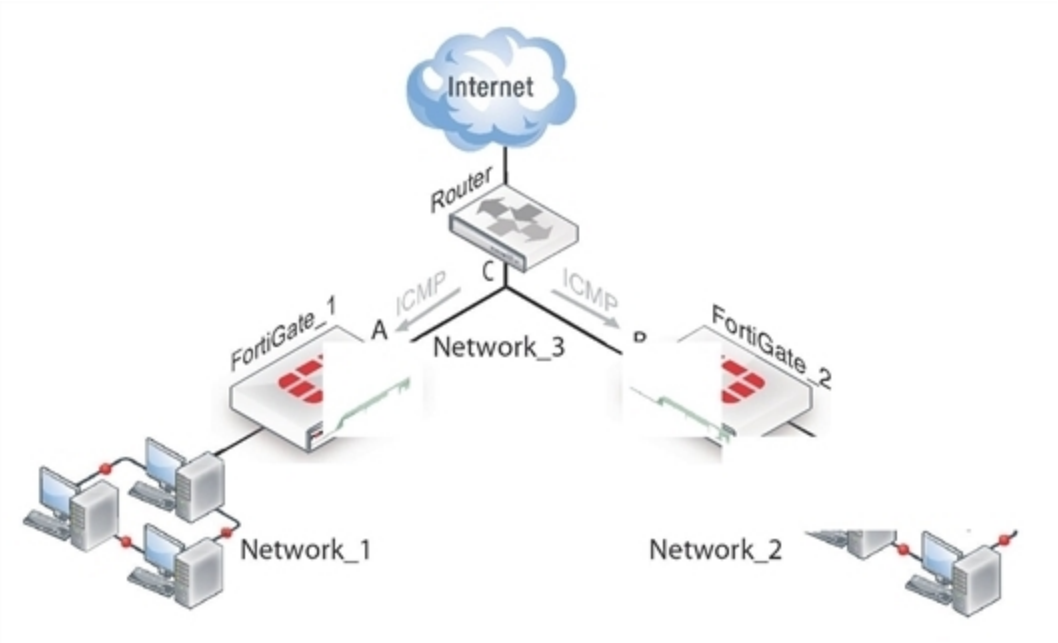
If you want to configure a VPN between two FortiGate units running in transparent mode, each unit must have an independent connection to a router that acts as a gateway to the Internet, and both units must be on separate networks that have a different address space. When the two networks linked by the VPN tunnel have different address spaces (see the figure below), at least one router must separate the two FortiGate units, unless the packets can be redirected using ICMP (as shown in the following figure).

Link between two FortiGate units in transparent mode



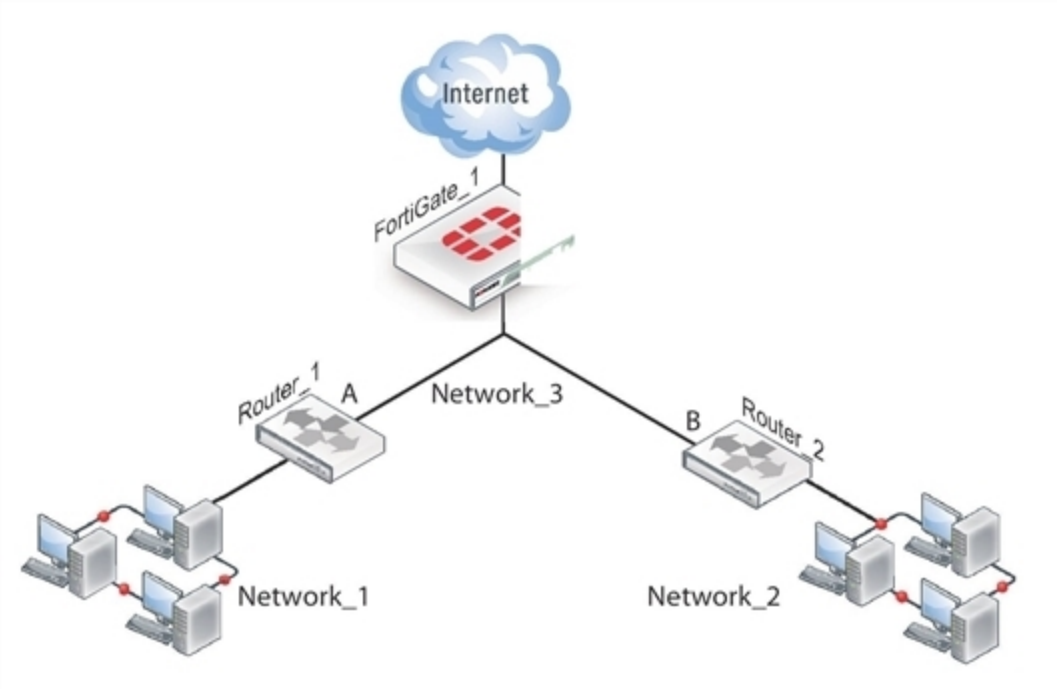
In the figure below, interface C behind the router is the default gateway for both FortiGate units. Packets that cannot be delivered on Network_1 are routed to interface C by default. Similarly, packets that cannot be delivered on Network_2 are routed to interface C. In this case, the router must be configured to redirect packets destined for Network_1 to interface A and redirect packets destined for Network_2 to interface B.

ICMP redirecting packets to two FortiGate units in transparent mode



If there are additional routers behind the FortiGate unit (see the figure below) and the destination IP address of an inbound packet is on a network behind one of those routers, the FortiGate routing table must include routes to those networks. For example, in the following figure, the FortiGate unit must be configured with static routes to interfaces A and B in order to forward packets to Network_1 and Network_2 respectively.

Destinations on remote networks behind internal routers



Transparent VPN infrastructure requirements

- The local FortiGate unit must be operating in transparent mode.
- The management IP address of the local FortiGate unit specifies the local VPN gateway. The management IP address is considered a static IP address for the local VPN peer.
- If the local FortiGate unit is managed through the Internet, or if the VPN peer connects through the Internet, the edge router must be configured to perform inbound NAT and forward management traffic and/or encrypted packets to the FortiGate unit.
- If the remote peer is operating in NAT mode, it must have a static public IP address.

A FortiGate unit operating in transparent mode requires the following basic configuration to operate as a node on the IP network:

- The unit must have sufficient routing information to reach the management station.
- For any traffic to reach external destinations, a default static route to an edge router that forwards packets to the Internet must be present in the FortiGate routing table.
- When all of the destinations are located on the external network, the FortiGate unit may route packets using a single default static route. If the network topology is more complex, one or more static routes in addition to the default static route may be required in the FortiGate routing table.

Only policy-based VPN configurations are possible in transparent mode.

Before you begin

An IPsec VPN definition links a gateway with a tunnel and an IPsec policy. If your network topology includes more than one virtual domain, you must choose components that were created in the same virtual domain. Therefore, before you define a transparent VPN configuration, choose an appropriate virtual domain in which to create the required interfaces, security policies, and VPN components. For more information, see the Virtual Domains guide.

Configure the VPN peers

1. The local VPN peer need to operate in transparent mode.
   To determine if your FortiGate unit is in transparent mode, go to **System > Dashboard > Status** to the **System Information** widget. Select **[change]**. Select transparent for the **Operation Mode**. Two new fields will appear to enter the **Management IP/Netmask**, and the **Default Gateway**.
   In transparent mode, the FortiGate unit is invisible to the network. All of its interfaces are on the same subnet and share the same IP address. You only have to configure a management IP address so that you can make configuration changes.

   The remote VPN peer may operate in NAT mode or transparent mode.
2. At the local FortiGate unit, define the Phase 1 parameters needed to establish a secure connection with the remote peer. See Phase 1 parameters on page 1581. Select **Advanced** and enter these settings in particular:

Remote Gateway	Select **Static IP Address**.
IP Address	Type the IP address of the public interface to the remote peer. If the remote peer is a FortiGate unit running in transparent mode, type the IP address of the remote management interface.
Advanced	Select **Nat-traversal**, and type a value into the **Keepalive Frequency** field. These settings protect the headers of encrypted packets from being altered by external NAT devices and ensure that NAT address mappings do not change while the VPN tunnel is open. For more information, see Phase 1 parameters on page 1581 and Phase 1 parameters on page 1581.

3. Define the Phase 2 parameters needed to create a VPN tunnel with the remote peer. See Phase 2 parameters on page 1598. Select the set of Phase 1 parameters that you defined for the remote peer. The name of the remote peer can be selected from the **Static IP Address** list.
4. Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See Defining VPN security policies on page 1603. Enter these settings in particular:
   - For the originating address (source address), enter the IP address and netmask of the private network behind the local peer network. for the management interface, for example, `10.10.10.0/24`. This address needs to be a range to allow traffic from your network through the tunnel. Optionally select `any` for this address.
   - For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer (for example, `192.168.10.0/24`). If the remote peer is a FortiGate unit running in transparent mode, enter the IP address of the remote management interface instead.
5. Define an IPsec security policy to permit communications between the source and destination addresses. See Defining VPN security policies on page 1603. Enter these settings in particular:

Incoming Interface	Select the local interface to the internal (private) network.
Source Address	Select the source address that you defined in Step 4.
Outgoing Interface	Select the interface to the edge router. When you configure the IPsec security policy on a remote peer that operates in NAT mode, you select the public interface to the external (public) network instead.
Destination Address	Select the destination address that you defined in Step 4.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 2 tunnel configuration that you created in Step 3 from the drop-down list. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

6. Place the policy in the policy list above any other policies having similar source and destination addresses.
7. Define another IPsec security policy to permit communications between the source and destination addresses in the opposite direction. This security policy and the previous one form a bi-directional policy pair. See Defining VPN security policies on page 1603. Enter these settings in particular:

Incoming Interface	Select the interface to the edge router. When you configure the IPsec security policy on a remote peer that operates in NAT mode, you select the public interface to the external (public) network instead.
Source Address	Select the destination address that you defined in Step 4..
Outgoing Interface	Select the local interface to the internal (private) network.
Destination Address	Select the source address that you defined in Step 4.
VPN Tunnel	Select **Use Existing** and select the name of the Phase 2 tunnel configuration that you created in Step 3 from the drop-down list. Select **Allow traffic to be initiated from the remote site** to enable traffic from the remote network to initiate the tunnel.

8. Repeat this procedure at the remote FortiGate unit to create bidirectional security policies. Use the local interface and address information local to the remote FortiGate unit.

For more information on transparent mode, see the System Administration Guide.

IPv6 IPsec VPNs

This chapter describes how to configure your FortiGate unit's IPv6 IPsec VPN functionality.

By default IPv6 configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable IPv6

1. Go to **System > Admin > Settings**.
2. In the **Display Options on GUI** section, select **IPv6**.
3. Select **Apply**.

The following topics are included in this section:

Overview of IPv6 IPsec support
Configuring IPv6 IPsec VPNs
Site-to-site IPv6 over IPv6 VPN example
Site-to-site IPv4 over IPv6 VPN example
Site-to-site IPv6 over IPv4 VPN example

Certificates

On a VPN with IPv6 Phase 1 configuration, you can authenticate using VPN certificates in which the common name (cn) is an IPv6 address. The `cn-type` keyword of the `user peer` command has an option, `ipv6`, to support this.

Overview of IPv6 IPsec support

FortiOS supports route-based IPv6 IPsec, but not policy-based. This section describes how IPv6 IPsec support differs from IPv4 IPsec support. FortiOS 5.2 is IPv6 Ready Logo Program Phase 2 certified.

Where both the gateways and the protected networks use IPv6 addresses, sometimes called IPv6 over IPv6, you can create either an auto-keyed or manually-keyed VPN. You can combine IPv6 and IPv4 addressing in an auto-keyed VPN in the following ways:

IPv4 over IPv6	The VPN gateways have IPv6 addresses. The protected networks have IPv4 addresses. The Phase 2 configurations at either end use IPv4 selectors.
IPv6 over IPv4	The VPN gateways have IPv4 addresses. The protected networks use IPv6 addresses. The Phase 2 configurations at either end use IPv6 selectors.

Compared with IPv4 IPsec VPN functionality, there are some limitations:

- Except for IPv6 over IPv4, remote gateways with Dynamic DNS are not supported.
- Selectors cannot be firewall address names. Only IP address, address range and subnet are supported.
- Redundant IPv6 tunnels are not supported.

Certificates

On a VPN with IPv6 Phase 1 configuration, you can authenticate using VPN certificates in which the common name (cn) is an IPv6 address. The `cn-type` keyword of the `user peer` command has an option, `ipv6`, to support this.

Configuring IPv6 IPsec VPNs

Configuration of an IPv6 IPsec VPN follows the same sequence as for an IPv4 route-based VPN: Phase 1 settings, Phase 2 settings, security policies and routing.

By default IPv6 configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable IPv6

1. Go to **System > Admin > Settings**.
2. In the **Display Options on GUI** section, select **IPv6**.
3. Select **Apply**.

Phase 1 configuration

In the web-based manager, you define the Phase 1 as IPv6 in the Advanced settings. Enable the IPv6 Version check box. You can then enter an IPv6 address for the remote gateway.

In the CLI, you define an IPsec Phase 1 configuration as IPv6 by setting `ip-version` to `6`. Its default value is `4`. Then, the `local-gw` and `remote-gw` keywords are hidden and the corresponding `local-gw6` and `remote-gw6` keywords are available. The values for `local-gw6` and `remote-gw6` must be IPv6 addresses. For example:

```
config vpn ipsec phase1-interface
   edit tunnel6
      set ip-version 6
      set remote-gw6 0:123:4567::1234
      set interface port3
      set proposal 3des-md5
   end
```

Phase 2 configuration

To create an IPv6 IPsec Phase 2 configuration in the web-based manager, you need to define IPv6 selectors in the Advanced settings. Change the default “0.0.0.0/0” address for Source address and Destination address to the IPv6 value “::/0”. If needed, enter specific IPv6 addresses, address ranges, or subnet addresses in these fields.

In the CLI, set `src-addr-type` and `dst-addr-type` to `ip6`, `range6` or `subnet6` to specify IPv6 selectors. By default, zero selectors are entered, “::/0” for the `subnet6` address type, for example. The simplest IPv6 Phase 2 configuration looks like this:

```
config vpn ipsec phase2-interface
   edit tunnel6_p2
```

```
        set phase1name tunnel6
        set proposal 3des-md5
        set src-addr-type subnet6
        set dst-addr-type subnet6
    end
```

The management of static selector rules is performed by the IKE daemon, which allows named selectors to be reloaded if any named address or address groups are changed, without requiring the FortiGate unit to be rebooted before applying changes.

Security policies

To complete the VPN configuration, you need a security policy in each direction to permit traffic between the protected network's port and the IPsec interface. You need IPv6 policies unless the VPN is IPv4 over IPv6.

Routing

Appropriate routing is needed for both the IPsec packets and the encapsulated traffic within them. You need a route, which could be the default route, to the remote VPN gateway via the appropriate interface. You also need a route to the remote protected network via the IPsec interface.

To create a static route in the web-based manager

1. Go to **Router > Static > Static Routes**.
   On low-end FortiGate units, go to **System > Network > Routing**.
2. Select the drop-down arrow on the **Create New** button and select **IPv6 Route**.
3. Enter the information and select **OK**.

In the CLI, use the `router static6` command. For example, where the remote network is fec0:0000:0000:0004::/64 and the IPsec interface is `toB`:

```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toB
      set dst fec0:0000:0000:0004::/64
   next
end
```

If the VPN is IPV4 over IPv6, the route to the remote protected network is an IPv4 route. If the VPN is IPv6 over IPv4, the route to the remote VPN gateway is an IPv4 route.

Site-to-site IPv6 over IPv6 VPN example

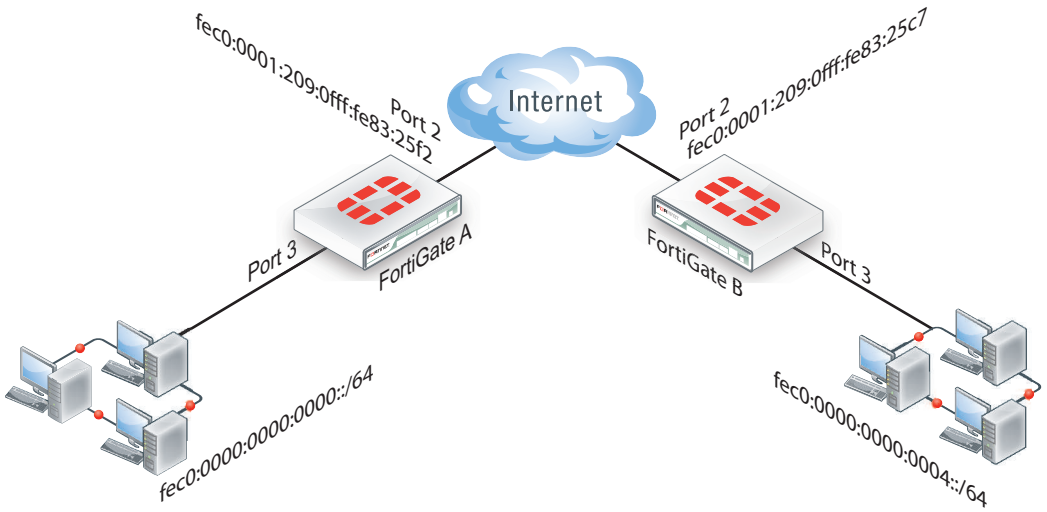
In this example, computers on IPv6-addressed private networks communicate securely over public IPv6 infrastructure.

By default IPv6 configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable IPv6

1. Go to **System > Admin > Settings**.
2. In the **Display Options on GUI** section, select **IPv6**.
3. Select **Apply**.

Example IPv6-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the public network and port 3 connects to the local network.

```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0001:209:0fff:fe83:25f2/64
      end
   next
   edit port3
      config ipv6
         set ip6-address fec0::0000:209:0fff:fe83:25f3/64
      end
   next
end
```

Configure FortiGate A IPsec settings

The Phase 1 configuration creates a virtual IPsec interface on port 2 and sets the remote gateway to the public IP address FortiGate B. This configuration is the same as for an IPv4 route-based VPN, except that `ip-version` is set to `6` and the `remote-gw6` keyword is used to specify an IPv6 remote gateway address.

```
config vpn ipsec phase1-interface
```

```
   edit toB
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
```

By default, Phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet6`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
   edit toB2
      set phase1name toB
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
```

Configure FortiGate A security policies

Security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. The address `all6` must be defined using the `firewall address6` command as `::/0`.

```
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toB
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toB
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB. A default route sends all IPv6 traffic out on port2.

```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
```

```
      set device toB
      set dst fec0:0000:0000:0004::/64
   end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. Security policies enable traffic to pass between the private network and the IPsec interface. Routing ensures traffic for the private network behind FortiGate A goes through the VPN and that all IPv6 packets are routed to the public network.

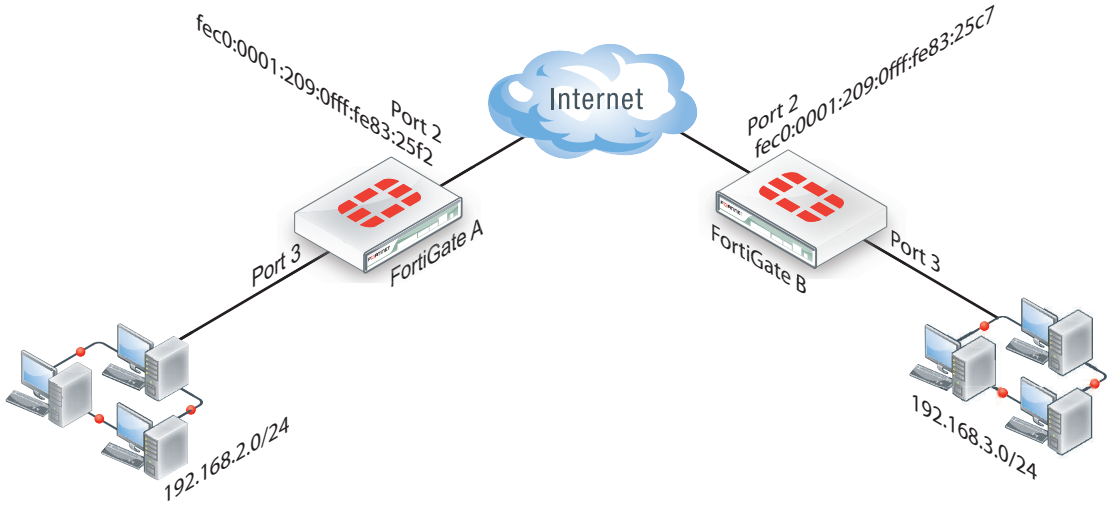
```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0003:209:0fff:fe83:25c7/64
      end
   next
   edit port3
      config ipv6
         set ip6-address fec0::0004:209:0fff:fe83:2569/64
      end
   end
config vpn ipsec phase1-interface
   edit toA
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toA
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toA
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
```

```
      set schedule always
   end
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toA
      set dst fec0:0000:0000:0000::/64
end
```

Site-to-site IPv4 over IPv6 VPN example

In this example, two private networks with IPv4 addressing communicate securely over IPv6 infrastructure.

Example IPv4-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv6 public network and port 3 connects to the IPv4 LAN.

```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0001:209:0fff:fe83:25f2/64
      end
   next
   edit port3
      set 192.168.2.1/24
   end
```

Configure FortiGate A IPsec settings

The Phase 1 configuration is the same as in the IPv6 over IPv6 example.

```
config vpn ipsec phase1-interface
   edit toB
      set ip-version 6
```

```
      set interface port2
      set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
```

The Phase 2 configuration is the same as you would use for an IPv4 VPN. By default, Phase 2 selectors are set to accept all subnet addresses for source and destination.

```
config vpn ipsec phase2-interface
   edit toB2
      set phase1name toB
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
   end
```

Configure FortiGate A security policies

Security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. These are IPv4 security policies.

```
config firewall policy
   edit 1
      set srcintf port3
      set dstintf toB
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toB
      set dstintf port3
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB using an IPv4 static route. A default route sends all IPv6 traffic, including the IPv6 IPsec packets, out on port2.

```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toB
      set dst 192.168.3.0/24
   end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. The IPsec Phase 2 configuration has IPv4 selectors.

IPv4 security policies enable traffic to pass between the private network and the IPsec interface. An IPv4 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv6 static route ensures that all IPv6 packets are routed to the public network.

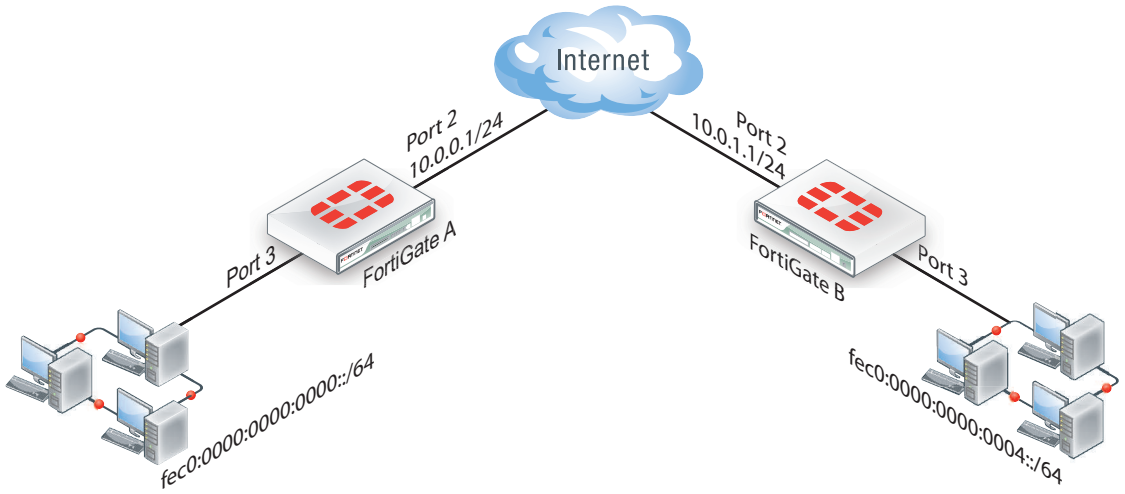
```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0003:fe83:25c7/64
      end
   next
   edit port3
      set 192.168.3.1/24
   end
config vpn ipsec phase1-interface
   edit toA
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
   end
config firewall policy
   edit 1
      set srcintf port3
      set dstintf toA
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toA
      set dstintf port3
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
   end
config router static6
   edit 1
      set device port2
```

```
      set dst 0::/0
   next
   edit 2
      set device toA
      set dst 192.168.2.0/24
   end
```

Site-to-site IPv6 over IPv4 VPN example

In this example, IPv6-addressed private networks communicate securely over IPv4 public infrastructure.

Example IPv6-over-IPv4 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv4 public network and port 3 connects to the IPv6 LAN.

```
config system interface
   edit port2
      set 10.0.0.1/24
      next
      edit port3
      config ipv6
         set ip6-address fec0::0001:209:0fff:fe83:25f3/64
      end
```

Configure FortiGate A IPsec settings

The Phase 1 configuration uses IPv4 addressing.

```
config vpn ipsec phase1-interface
   edit toB
      set interface port2
      set remote-gw 10.0.1.1
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
```

The Phase 2 configuration uses IPv6 selectors. By default, Phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet6`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
   edit toB2
      set phase1name toB
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
```

Configure FortiGate A security policies

IPv6 security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. Define the address `all6` using the `firewall address6` command as `::/0`.

```
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toB
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toB
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB using an IPv6 static route. A default route sends all IPv4 traffic, including the IPv4 IPsec packets, out on port2.

```
config router static6
      edit 1
         set device toB
         set dst fec0:0000:0000:0004::/64
      end
   config router static
      edit 1
         set device port2
         set dst 0.0.0.0/0
         set gateway 10.0.0.254
      end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the IPv4 public IP address of FortiGate A. The IPsec Phase 2 configuration has IPv6 selectors.

IPv6 security policies enable traffic to pass between the private network and the IPsec interface. An IPv6 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv4 static route ensures that all IPv4 packets are routed to the public network.

```
config system interface
   edit port2
      set 10.0.1.1/24
   next
   edit port3
      config ipv6
         set ip6-address fec0::0004:209:0fff:fe83:2569/64
      end
config vpn ipsec phase1-interface
   edit toA
      set interface port2
      set remote-gw 10.0.0.1
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toA
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toA
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
config router static6
   edit 1
      set device toA
```

```
      set dst fec0:0000:0000:0000::/64
   end
config router static
   edit 1
      set device port2
      set gateway 10.0.1.254
   end
```

L2TP and IPsec (Microsoft VPN)

This section describes how to set up a VPN that is compatible with the Microsoft Windows native VPN, which is Layer 2 Tunneling Protocol (L2TP) with IPsec encryption.

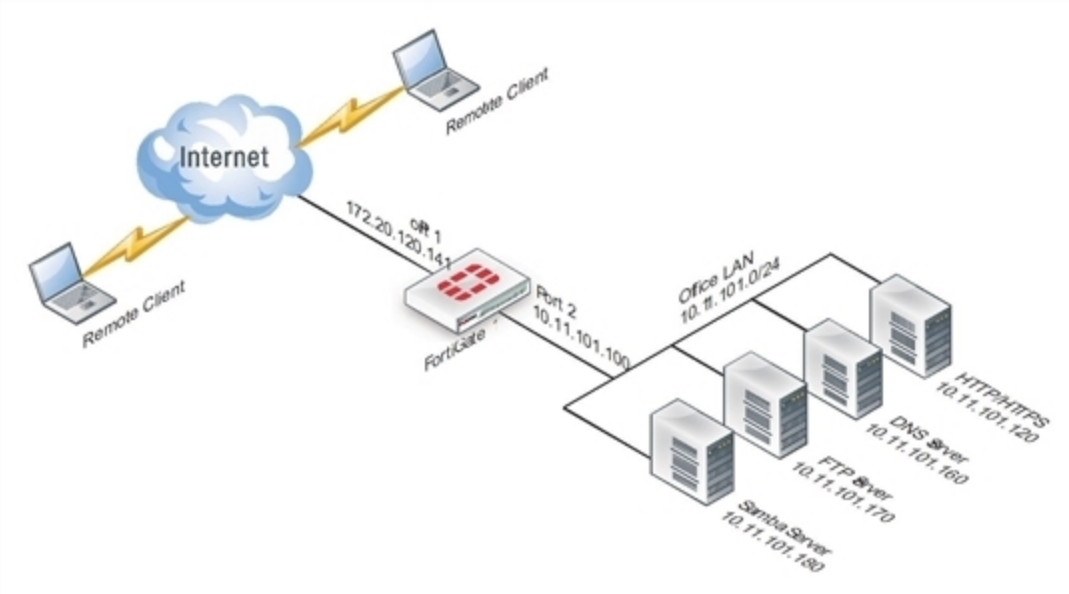
The following topics are included in this section:

Overview
Assumptions
Configuring the FortiGate unit
Configuring the Windows PC
Troubleshooting

Overview

The topology of a VPN for Microsoft Windows dialup clients is very similar to the topology for FortiClient Endpoint Security clients.

Example FortiGate VPN configuration with Microsoft clients



For users, the difference is that instead of installing and using the FortiClient application, they configure a network connection using the software built into the Microsoft Windows operating system. FortiOS 5.2 can configure a FortiGate unit to work with unmodified Microsoft VPN client software.

Layer 2 Tunneling Protocol (L2TP)

L2TP is a tunneling protocol published in 1999 that is used with VPNs, as the name suggests. Microsoft Windows operating system has a built-in L2TP client starting since Windows 2000. Mac OS X 10.3 system and higher also have a built-in client.

L2TP provides no encryption and used UDP port 1701. IPsec is used to secure L2TP packets. The initiator of the L2TP tunnel is called the L2TP Access Concentrator (LAC).

L2TP and IPsec is supported for native Windows XP, Windows Vista and Mac OSX native VPN clients. However, in Mac OSX (OSX 10.6.3, including patch releases) the L2TP feature does not work properly on the Mac OS side.

Assumptions

The following assumptions have been made for this example:

- L2TP protocol traffic is allowed through network firewalls (TCP and UDP port 1701)
- User has Microsoft Windows 2000 or higher — a Windows version that supports L2TP

Configuring the FortiGate unit

To configure the FortiGate unit, you must:

- Configure LT2P users and firewall user group.
- Configure the L2TP VPN, including the IP address range it assigns to clients.
- Configure an IPsec VPN with encryption and authentication settings that match the Microsoft VPN client.
- Configure security policies.

Configuring LT2P users and firewall user group

Remote users must be authenticated before they can request services and/or access network resources through the VPN. The authentication process can use a password defined on the FortiGate unit or an established external authentication mechanism such as RADIUS or LDAP.

Creating user accounts

You need to create user accounts and then add these users to a firewall user group to be used for L2TP authentication. The Microsoft VPN client can automatically send the user's Window network logon credentials. You might want to use these for their L2TP user name and password.

To create a user account - web-based manager

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Enter the **User Name**.
3. Do one of the following:
   - Select **Password** and enter the user's assigned password.
   - Select **Match user on LDAP server**, **Match user on RADIUS server**, or **Match user onTACACS+ server** and select the authentication server from the list. The authentication server must be already configured on the FortiGate unit.
4. Select **OK**.

To create a user account - CLI

To create a user account called `user1` with the password `123_user`, enter:

```
config user local
   edit user1
      set type password
```

```
      set passwd "123_user"
      set status enable
   end
```

Creating a user group

When clients connect using the L2TP-over-IPsec VPN, the FortiGate unit checks their credentials against the user group you specify for L2TP authentication. You need to create a firewall user group to use for this purpose.

To create a user group - web-based manager

1. Go to **User & Device > User > User Groups**, select **Create New**, and enter the following:

Name	Type or edit the user group name (for example, `L2TP_group`).
Type	Select **Firewall**.
Available Users/Groups	The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that can be added to the user group. To add a member to this list, select the name and then select the right arrow button.
Members	The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that belong to the user group. To remove a member, select the name and then select the left arrow button.

2. Select **OK**.

To create a user group - CLI

To create the user group L2TP_group and add members User_1, User_2, and User_3, enter:

```
config user group
   edit L2TP_group
      set group-type firewall
      set member User_1 User_2 User_3
   end
```

Configuring L2TP

You can only configure L2TP settings in the CLI. As well as enabling L2TP, you set the range of IP address values that are assigned to L2TP clients and specify the user group that can access the VPN. For example, to allow access to users in the L2TP_group and assign them addresses in the range 192.168.0.50 to 192.168.0.59, enter:

```
config vpn l2tp
   set sip 192.168.0.50
   set eip 192.168.0.59
   set status enable
   set usrgrp "L2TP_group"
end
```

One of the security policies for the L2TP over IPsec VPN uses the client address range, so you need also need to create a firewall address for that range. For example,

```
config firewall address
   edit L2TPclients
      set type iprange
```

```
        set start-ip 192.168.0.50
        set end-ip 192.168.0.59
    end
```

Alternatively, you could define this range in the web-based manager.

Configuring IPsec

The Microsoft VPN client uses IPsec for encryption. The configuration needed on the FortiGate unit is the same as for any other IPsec VPN with the following exceptions.

- Transport mode is used instead of tunnel mode.
- The encryption and authentication proposals must be compatible with the Microsoft client.

L2TP over IPsec is supported on the FortiGate unit using policy-based, not route-based configurations.

When configuring L2TP, do not name the VPN as "L2TP" as that will result in a conflict.

Configuring Phase 1 - web-based manager

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the **Convert to Custom Tunnel** button).

Name	Enter a name for this VPN, dialup_p1 for example.
Remote Gateway	**Dialup User**
Local Interface	Select the network interface that connects to the Internet. For example, port1.
Mode	**Main (ID protection)**
Authentication Method	**Preshared Key**
Pre-shared Key	Enter the preshared key. This key must also be entered in the Microsoft VPN client.
Advanced	Select **Advanced** to enter the following information.
Phase 1 Proposal	Enter the following Encryption/Authentication pairs: AES256-MD5, 3DES-SHA1, AES192-SHA1
Diffie-Hellman Group	2
NAT Traversal	Enable
Dead Peer Detection	Enable

Configuring Phase 1 - CLI

To create a Phase 1 configuration called dialup_p1 on a FortiGate unit that has port1 connected to the Internet, you would enter:

```
config vpn ipsec phase1
   edit dialup_p1
      set type dynamic
      set interface port1
      set mode main
      set psksecret ********
      set proposal aes256-md5 3des-sha1 aes192-sha1
      set dhgrp 2
      set nattraversal enable
      set dpd enable
end
```

Configuring Phase 2 - web-based manager

1. Open the **Phase 2 Selectors** panel.
2. Enter the following information and then select **OK**.

Phase 2 Proposal	Enter the following Encryption/Authentication pairs: AES256-MD5, 3DES-SHA1, AES192-SHA1
Enable replay detection	Enable
Enable perfect forward secrecy (PFS)	Disable
Keylife	3600 seconds

3. Make this a transport-mode VPN. You must use the CLI to do this. If your Phase 2 name is dialup_p2, you would enter:

```
config vpn ipsec phase2
   edit dialup_p2
      set encapsulation transport-mode
   end
```

Configuring Phase 2 - CLI

To configure a Phase 2 to work with your phase_1 configuration, you would enter:

```
config vpn ipsec phase2
   edit dialup_p2
      set phase1name dialup_p1
      set proposal aes256-md5 3des-sha1 aes192-sha1
      set replay enable
      set pfs disable
      set keylifeseconds 3600
      set encapsulation transport-mode
   end
```

Configuring security policies

The security policies required for L2TP over IPsec VPN are:

- An IPsec policy, as you would create for any policy-based IPsec VPN
- A regular ACCEPT policy to allow traffic from the L2TP clients to access the protected network

Configuring the IPsec security policy - web-based manager

1. Go to **System > Config > Features** and enable **Policy-based IPsec VPN**.
2. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
3. Set the **Action** to **IPsec** and enter the following information:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	All
Outgoing Interface	Select the FortiGate unit's public interface.
Destination Address	All
VPN Tunnel	Select **Use Existing** and select the name of the Phase 1 configuration that you created. For example, dialup_p1. See Configuring IPsec on page 1733.
Allow traffic to be initiated from the remote site	enable

4. Select **OK**.

Configuring the IPsec security policy - CLI

If your VPN tunnel (Phase 1) is called dialup_p1, your protected network is on port2, and your public interface is port1, you would enter:

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action ipsec
      set schedule always
      set service all
      set inbound enable
      set vpntunnel dialup_p1
   end
```

Configuring the ACCEPT security policy - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and leave the **Policy Subtype** as **Address**.
3. Enter the following information and select **OK**:

Incoming Interface	Select the FortiGate unit's public interface.
Source Address	Select the firewall address that you defined for the L2TP clients.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	All
Action	ACCEPT

Configuring the ACCEPT security policy - CLI

If your public interface is port1, your protected network is on port2, and L2TPclients is the address range that L2TP clients use, you would enter:

```
config firewall policy
   edit 1
      set srcintf port1
      set dstintf port2
      set srcaddr L2TPclients
      set dstaddr all
      set action accept
      set schedule always
      set service all
   end
```

Configuring the Windows PC

Configuration of the Windows PC for a VPN connection to the FortiGate unit consists of the following:

1. In Network Connections, configure a Virtual Private Network connection to the FortiGate unit.
2. Ensure that the IPSEC service is running.
3. Ensure that IPsec has not been disabled for the VPN client. It may have been disabled to make the Microsoft VPN compatible with an earlier version of FortiOS.

The instructions in this section are based on Windows XP SP3. Other versions of Windows may vary slightly.

To configure the network connection

1. Open **Network Connections**.
   This is available through the Control Panel.
2. Double-click **New Connection Wizard** and **Select Next**.
3. Select **Connect to the network at my workplace**.
4. Select **Next**.
5. Select **Virtual Private Network connection** and select **Next**.
6. In the **Company Name** field, enter a name for the connection and select **Next**.
7. Select **Do not dial the initial connection** and then select **Next**.
8. Enter the public IP address or FQDN of the FortiGate unit and select **Next**.
9. Optionally, select **Add a shortcut to this connection to my desktop**.
10. Select **Finish**.
    The **Connect** dialog opens on the desktop.

11. Select **Properties** and then select the **Security** tab.
12. Select **IPsec Settings**.
13. Select **Use pre-shared key for authentication**, enter the preshared key that you configured for your VPN, and select **OK**.
14. Select **OK**.

To check that the IPSEC service is running

1. Open **Administrative Tools** through the Control Panel.
2. Double-click **Services**.
3. Look for IPSEC Services. Confirm that the **Startup Type** is **Automatic** and **Status** is set to **Started**. If needed, double-click **IPSEC Services** to change these settings.

To check that IPsec has not been disabled

1. Select **Start > Run**.
2. Enter regedit and select **OK**.
3. Find the Registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
4. If there is a ProhibitIPsec value, it must be set to 0.

Troubleshooting

This section describes some checks and tools you can use to resolve issues with L2TP-over-IPsec VPNs.

This section includes:

- Quick checks
- Mac OS X and L2TP
- Setting up logging
- Using the FortiGate unit debug commands

Quick checks

The table below is a list of common L2TP over IPsec VPN problems and the possible solutions.

Problem	What to check
IPsec tunnel does not come up.	Check the logs to determine whether the failure is in Phase 1 or Phase 2. Check the settings, including encapsulation setting, which must be transport-mode. Check the user password. Confirm that the user is a member of the user group assigned to L2TP. On the Windows PC, check that the IPsec service is running and has not been disabled. See Troubleshooting on page 1737.
Tunnel connects, but there is no communication.	Did you create an ACCEPT security policy from the public network to the protected network for the L2TP clients? See Troubleshooting on page 1737.

Mac OS X and L2TP

FortiOS allows L2TP connections with empty AVP host names and therefore Mac OS X L2TP connections can connect to the FortiGate.

Previously, FortiOS refused L2TP connections with empty AVP host names in compliance with RFC 2661 and RFC 3931.

Setting up logging

L2TP logging must be enabled to record L2TP events. Alert email can be configured to report L2TP errors.

To configure FortiGate logging for L2TP over IPsec

1. Go to **Log & Report > Log Config > Log Settings**.
2. Select **Event Log**.
3. Select the **VPN activity event** check box.
4. Select **Apply**.

To view FortiGate logs

1. Go to **Log & Report > Event Log > VPN**.
2. Select the **Log location** if required.
3. After each attempt to start the L2TP over IPsec VPN, select **Refresh** to view logged events.

Using the FortiGate unit debug commands

To view debug output for IKE and L2TP

1. Start an SSH or Telnet session to your FortiGate unit.
2. Enter the following CLI commands

```
diagnose debug application ike -1
diagnose debug application l2tp -1
diagnose debug enable
```

3. Attempt to use the VPN and note the debug output in the SSH or Telnet session.
4. Enter the following command to reset debug settings to default:

```
diagnose debug reset
```

To use the packet sniffer

1. Start an SSH or Telnet session to your FortiGate unit.
2. Enter the following CLI command

```
diagnose sniffer packet any icmp 4
```

3. Attempt to use the VPN and note the debug output.
4. Enter `Ctrl-C` to end sniffer operation.

Typical L2TP over IPsec session startup log entries - raw format

```
2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 1" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1" status=success init=remote mode=main dir=outbound stage=1
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 1" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1" status=success init=remote mode=main dir=outbound stage=2
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 1" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1" status=success init=remote mode=main dir=inbound stage=3
role=responder result=DONE

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 1" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1_0" status=success init=remote mode=main dir=outbound stage=3
role=responder result=DONE

2010-01-11 16:39:58 log_id=0101037129 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 2" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1_0" status=success init=remote mode=quick dir=outbound stage=1
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037133 type=event subtype=ipsec pri=notice vd="root" msg="install IPsec
SA" action="install_sa" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1_0" role=responder in_spi=61100fe2 out_spi=bd70fca1

2010-01-11 16:39:58 log_id=0101037139 type=event subtype=ipsec pri=notice vd="root" msg="IPsec Phase 2
status change" action="phase2-up" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A"
xauth_group="N/A" vpn_tunnel="dialup_p1_0" phase2_name=dialup_p2

2010-01-11 16:39:58 log_id=0101037138 type=event subtype=ipsec pri=notice vd="root" msg="IPsec
connection status change" action="tunnel-up" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500
loc_port=500 out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_
user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0" tunnel_ip=172.20.120.151 tunnel_id=1552003005
tunnel_type=ipsec duration=0 sent=0 rcvd=0 next_stat=0 tunnel=dialup_p1_0

2010-01-11 16:39:58 log_id=0101037129 type=event subtype=ipsec pri=notice vd="root" msg="progress IPsec
Phase 2" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
```

```
group="N/A" vpn_tunnel="dialup_p1_0" status=success init=remote mode=quick dir=inbound stage=2
role=responder result=DONE

2010-01-11 16:39:58 log_id=0101037122 type=event subtype=ipsec pri=notice vd="root" msg="negotiate IPsec
Phase 2" action="negotiate" rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500 out_
intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A" xauth_user="N/A" xauth_
group="N/A" vpn_tunnel="dialup_p1_0" status=success role=responder esp_transform=ESP_3DES esp_auth=HMAC_
SHA1

2010-01-11 16:39:58 log_id=0103031008 type=event subtype=ppp vd=root pri=information action=connect
status=success msg="Client 172.20.120.151 control connection started (id 805), assigned ip 192.168.0.50"

2010-01-11 16:39:58 log_id=0103029013 type=event subtype=ppp vd=root pri=notice pppd is started

2010-01-11 16:39:58 log_id=0103029002 type=event subtype=ppp vd=root pri=notice user="user1"
local=172.20.120.141 remote=172.20.120.151 assigned=192.168.0.50 action=auth_success msg="User 'user1'
using l2tp with authentication protocol MSCHAP_V2, succeeded"

2010-01-11 16:39:58 log_id=0103031101 type=event subtype=ppp vd=root pri=information action=tunnel-up
tunnel_id=1645784497 tunnel_type=l2tp remote_ip=172.20.120.151 tunnel_ip=192.168.0.50 user="user1"
group="L2TPusers" msg="L2TP tunnel established"
```

GRE over IPsec (Cisco VPN)

This section describes how to configure a FortiGate VPN that is compatible with Cisco-style VPNs that use GRE in an IPsec tunnel.

The following topics are included in this section:

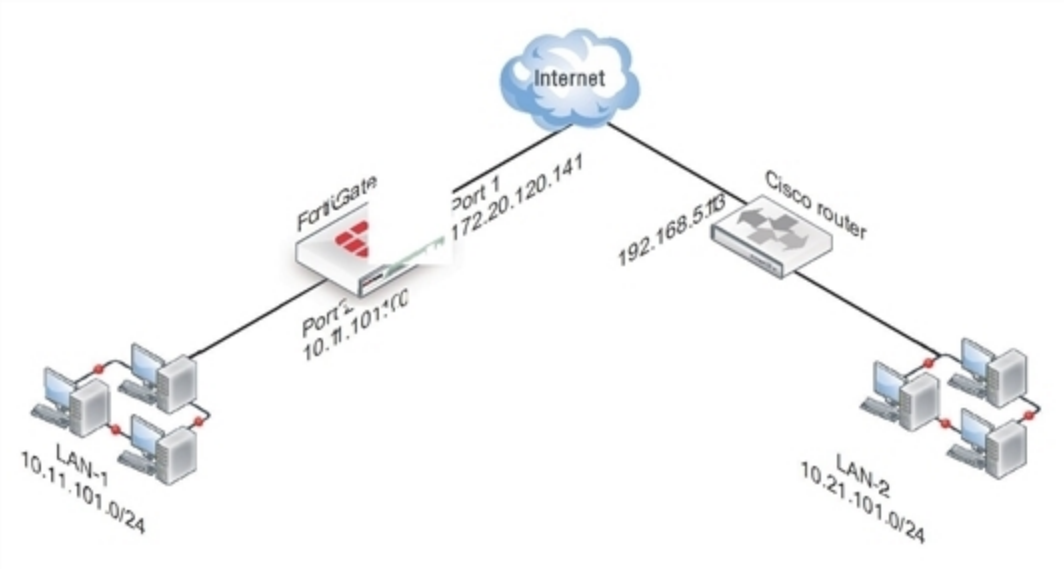
Overview
Configuring the FortiGate unit
Configuring the Cisco router
Troubleshooting

Overview

Cisco products that include VPN support often use Generic Routing Encapsulation (GRE) protocol tunnel over IPsec encryption. This chapter describes how to configure a FortiGate unit to work with this type of Cisco VPN.

Cisco VPNs can use either transport mode or tunnel mode IPsec. Previously, the FortiGate unit was compatible only with tunnel mode IPsec.

Example FortiGate to Cisco GRE-over-IPsec VPN



In this example, users on LAN-1 are provided access to LAN-2.

Configuring the FortiGate unit

There are several steps to the GRE-over-IPsec configuration:

- Enable overlapping subnets. This is needed because the IPsec and GRE tunnels will use the same addresses.
- Configure a route-based IPsec VPN on the external interface.
- Configure a GRE tunnel on the virtual IPsec interface. Set its local gateway and remote gateway addresses to match the local and remote gateways of the IPsec tunnel.

- Configure security policies to allow traffic to pass in both directions between the GRE virtual interface and the IPsec virtual interface.
- Configure security policies to allow traffic to pass in both directions between the protected network interface and the GRE virtual interface.
- Configure a static route to direct traffic destined for the network behind the Cisco router into the GRE-over-IPsec tunnel.

Enabling overlapping subnets

By default, each FortiGate unit network interface must be on a separate network. The configuration described in this chapter assigns an IPsec tunnel end point and the external interface to the same network. Enable subnet overlap as follows:

```
config system settings
   set allow-subnet-overlap enable
end
```

Configuring the IPsec VPN

A route-based VPN is required. It must use encryption and authentication algorithms compatible with the Cisco equipment to which it connects. In this chapter, preshared key authentication is shown.

To configure the IPsec VPN - web-based manager

1. Define the Phase 1 configuration needed to establish a secure connection with the remote Cisco device. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel, tocisco for example. This is the name of the virtual IPsec interface. It appears in Phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	For example, 192.168.16.128.
IP Address	Enter the IP address of the Cisco device public interface. For example, 192.168.16.128.
Local Interface	Select the FortiGate unit's public interface. For example, 172.20.120.141.
Mode	Select **Main (ID Protection)**.
Authentication Method	**Preshared Key**
Pre-shared Key	Enter the preshared key. It must match the preshared key on the Cisco device.
Advanced	Select the Advanced button to see the following settings.
Phase 1 Proposal	**3DES-MD5** At least one proposal must match the settings on the Cisco unit.

For more information about these settings, see Phase 1 parameters on page 1581.

2. Define the Phase 2 parameters needed to create a VPN tunnel with the remote peer. For compatibility with the Cisco router, Quick Mode Selectors must be entered, which includes specifying protocol 47, the GRE protocol. Enter these settings in particular:

Phase 2 Proposal	**3DES-MD5** At least one proposal must match the settings on the Cisco unit.
Quick Mode Selector	
Source Address	Enter the GRE local tunnel end IP address. For example 172.20.120.141.
Source Port	0
Destination Address	Enter the GRE remote tunnel end IP address. For example 192.168.16.128.
Destination Port	0
Protocol	47

   For more information about these settings, see Phase 2 parameters on page 1598.

3. If the Cisco device is configured to use transport mode IPsec, you need to use transport mode on the FortiGate VPN. You can configure this only in the CLI. In your Phase 2 configuration, set `encapsulation` to `transport-mode` as follows:

```
config vpn phase2-interface
   edit to_cisco_p2
      set encapsulation transport-mode
   end
```

To configure the IPsec VPN - CLI

```
config vpn ipsec phase1-interface
   edit tocisco
      set interface port1
      set proposal 3des-sha1 aes128-sha1
      set remote-gw 192.168.16.128
      set psksecret xxxxxxxxxxxxxxx
   end
config vpn ipsec phase2-interface
   edit tocisco_p2
      set phase1name "tocisco"
      set proposal 3des-md5
      set encapsulation tunnel-mode // if tunnel mode
      set encapsulation transport-mode // if transport mode
      set protocol 47
      set src-addr-type ip
      set dst-start-ip 192.168.16.128
      set src-start-ip 172.20.120.141
   end
```

Adding IPsec tunnel end addresses

The Cisco configuration requires an address for its end of the IPsec tunnel. The addresses are set to match the GRE gateway addresses. Use the CLI to set the addresses, like this:

```
config system interface
   edit tocisco
      set ip 172.137.0.1 255.255.255.255
      set remote-ip 172.128.0.1
   end
```

Configuring the GRE tunnel

The GRE tunnel runs between the virtual IPsec public interface on the FortiGate unit and the Cisco router. You must use the CLI to configure a GRE tunnel. In the example, you would enter:

```
config system gre-tunnel
   edit gre1
      set interface tocisco
      set local-gw 172.137.0.1
      set remote-gw 172.128.0.1
end
```

`interface` is the virtual IPsec interface, `local-gw` is the FortiGate unit public IP address, and `remote-gw` is the remote Cisco device public IP address

Adding GRE tunnel end addresses

You will also need to add tunnel end addresses. The Cisco router configuration requires an address for its end of the GRE tunnel. Using the CLI, enter tunnel end addresses that are not used elsewhere on the FortiGate unit, like this:

```
config system interface
   edit gre1
      set ip 10.0.1.1 255.255.255.255
      set remote-ip 10.0.1.2
   end
```

Configuring security policies

Two sets of security policies are required:

- Policies to allow traffic to pass in both directions between the GRE virtual interface and the IPsec virtual interface.
- Policies to allow traffic to pass in both directions between the protected network interface and the GRE virtual interface.

To configure security policies - web-based manager

1. Define an ACCEPT firewall security policy to permit communications between the protected network and the GRE tunnel:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	**All**

Outgoing Interface	Select the GRE tunnel virtual interface you configured.
Destination Address	**All**
Action	**ACCEPT**
Enable NAT	Disable

2. To permit the remote client to initiate communication, you need to define a firewall address security policy for communication in that direction:

Incoming Interface	Select the GRE tunnel virtual interface you configured.
Source Address	**All**
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	**All**
Action	**ACCEPT**
Enable NAT	Disable

3. Define a pair of ACCEPT firewall address security policies to permit traffic to flow between the GRE virtual interface and the IPsec virtual interface:

Incoming Interface	Select the GRE virtual interface. See Configuring the GRE tunnel on page 1744.
Source Address	**All**
Outgoing Interface	Select the virtual IPsec interface you created. See Configuring the IPsec VPN on page 1742.
Destination Address	**All**
Action	**ACCEPT**
Enable NAT	Disable

Incoming Interface	Select the virtual IPsec interface you created. See Configuring the IPsec VPN on page 1742.
Source Address	**All**
Outgoing Interface	Select the GRE virtual interface.See Configuring the GRE tunnel on page 1744.
Destination Address	**All**

Action	**ACCEPT**
Enable NAT	Disable

To configure security policies - CLI

```
config firewall policy
   edit 1 // LAN to GRE tunnel
      set srcintf port2
      set dstintf gre1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 2 // GRE tunnel to LAN
      set srcintf gre1
      set dstintf port2
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
   next
   edit 3 // GRE tunnel to IPsec interface
      set srcintf "gre1"
      set dstintf "tocisco"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
   next
   edit 4 // IPsec interface to GRE tunnel
      set srcintf "tocisco"
      set dstintf "gre1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
   end
```

Configuring routing

Traffic destined for the network behind the Cisco router must be routed to the GRE tunnel. To do this, create a static route

1. Go to **Router > Static > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the following information and select **OK**.

Destination IP/Mask	Enter the IP address and netmask for the network behind the Cisco router. For example 10.21.101.0 255.255.255.0.
Device	Select the GRE virtual interface.
Distance (Advanced)	Leave setting at default value.

In the CLI, using the example values, you would enter

```
config router static
   edit 0
      set device gre1
      set dst 10.21.101.0 255.255.255.0
   end
```

Configuring the Cisco router

Using Cisco IOS, you would configure the Cisco router as follows, using the addresses from the example:

```
config ter
crypto ipsec transform-set myset esp-3des esp-md5-hmac
no mode
exit
no ip access-list extended tunnel
ip access-list extended tunnel
permit gre host 192.168.5.113 host 172.20.120.141
exit
interface Tunnel1
ip address 10.0.1.2 255.255.255.0
tunnel source 192.168.5.113
tunnel destination 172.20.120.141
!
ip route 10.11.101.0 255.255.255.0 Tunnel1
end
clea crypto sa
clea crypto isakmp
```

For transport mode, change `no mode` to `mode transport`.

This is only the portion of the Cisco router configuration that applies to the GRE-over-IPsec tunnel. For more information, refer to the Cisco documentation.

Troubleshooting

This section describes some checks and tools you can use to resolve issues with the GRE-over-IPsec VPN.

Quick checks

Here is a list of common problems and what to verify.

Problem	What to check
No communication with remote network.	Use the `execute ping` command to ping the Cisco device public interface. Use the FortiGate VPN Monitor page to see whether the IPsec tunnel is up or can be brought up.
IPsec tunnel does not come up.	Check the logs to determine whether the failure is in Phase 1 or Phase 2. Check that the encryption and authentication settings match those on the Cisco device. Check the encapsulation setting: tunnel-mode or transport-mode. Both devices must use the same mode.
Tunnel connects, but there is no communication.	Check the security policies. See Troubleshooting on page 1747. Check routing. See Troubleshooting on page 1747.

Setting up logging

To configure FortiGate logging for IPsec

1. Go to **Log & Report > Log Config > Log Settings**.
2. Select the **Event Logging**.
3. Select **VPN activity event**.
4. Select **Apply**.

To view FortiGate logs

1. Go to **Log & Report > Event Log > VPN**.
2. Select the log storage type.
3. Select **Refresh** to view any logged events.

GRE tunnel keepalives

In the event that each GRE tunnel endpoint has keepalive enabled, firewall policies allowing GRE are required in both directions. The policy should be configured as follows (where the IP addresses and interface names are for example purposes only):

```
config firewall policy
   edit < id >
      set srcintf "gre"
      set dstintf "port1"
      set srcaddr "1.1.1.1"
      set dstaddr "2.2.2.2"
      set action accept
      set schedule "always"
      set service "GRE"
   next
end
```

GRE tunnel with multicast traffic

If you want multicast traffic to traverse the GRE tunnel, you need to configure a multicast policy as well as enable multicast forwarding.

- To configure a multicast policy, use the `config firewall multicast-policy` command.
- To enable multicast forwarding, use the following commands:

```
config system settings
   set multicast-forward enable
end
```

Using diagnostic commands

There are some diagnostic commands that can provide useful information. When using diagnostic commands, it is best practice that you connect to the CLI using a terminal program, such as puTTY, that allows you to save output to a file. This will allow you to review the data later on at your own speed without worry about missed data as the diag output scrolls by.

To use the packet sniffer

1. Enter the following CLI command:
   ```
   diag sniff packet any icmp 4
   ```
2. Ping an address on the network behind the FortiGate unit from the network behind the Cisco router.

   The output will show packets coming in from the GRE interface going out of the interface that connects to the protected network (LAN) and vice versa. For example:
   ```
   114.124303 gre1 in 10.0.1.2 -> 10.11.101.10: icmp: echo request
   114.124367 port2 out 10.0.1.2 -> 10.11.101.10: icmp: echo request
   114.124466 port2 in 10.11.101.10 -> 10.0.1.2: icmp: echo reply
   114.124476 gre1 out 10.11.101.10 -> 10.0.1.2: icmp: echo reply
   ```
3. Enter `CTRL-C` to stop the sniffer.

To view debug output for IKE

1. Enter the following CLI commands
   ```
   diagnose debug application ike -1
   diagnose debug enable
   ```
2. Attempt to use the VPN or set up the VPN tunnel and note the debug output.
3. Enter CTRL-C to stop the debug output.
4. Enter the following command to reset debug settings to default:
   ```
   diagnose debug reset
   ```

Protecting OSPF with IPsec

For enhanced security, OSPF dynamic routing can be carried over IPsec VPN links.

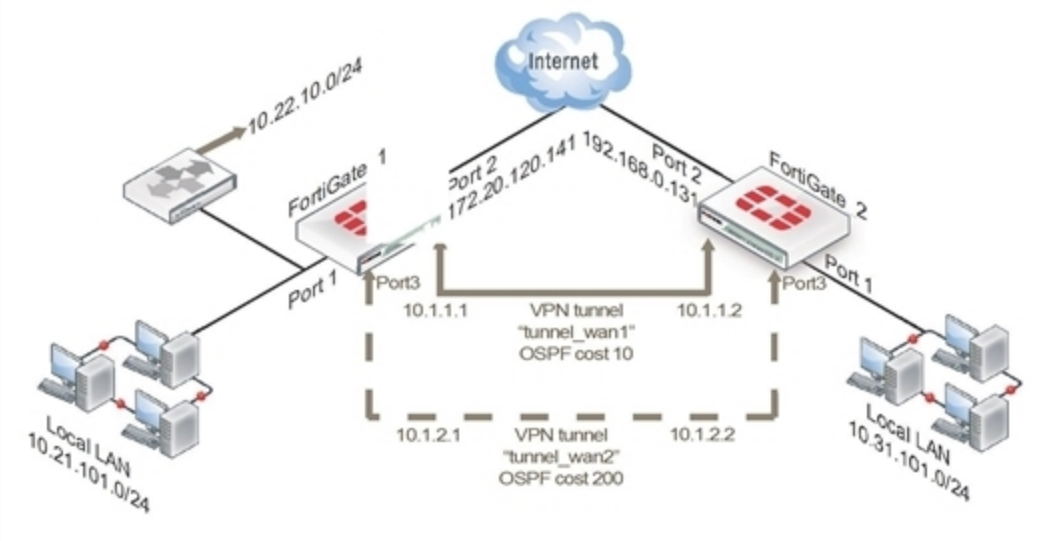
The following topics are included in this section:

Overview
OSPF over IPsec configuration
Creating a redundant configuration

Overview

This chapter shows an example of OSPF routing conducted over an IPsec tunnel between two FortiGate units. The network shown below is a single OSPF area. FortiGate_1 is an Area border router that advertises a static route to 10.22.10.0/24 in OSPF. FortiGate_2 advertises its local LAN as an OSPF internal route.

OSPF over an IPsec VPN tunnel



The section Overview describes the configuration with only one IPsec VPN tunnel, tunnel_wan1. Then, the section Overview describes how you can add a second tunnel to provide a redundant backup path. This is shown above as VPN tunnel “tunnel_wan2”.

Only the parts of the configuration concerned with creating the IPsec tunnel and integrating it into the OSPF network are described. It is assumed that security policies are already in place to allow traffic to flow between the interfaces on each FortiGate unit.

OSPF over IPsec configuration

There are several steps to the OSPF-over-IPsec configuration:

- Configure a route-based IPsec VPN on an external interface. It will connect to a corresponding interface on the other FortiGate unit. Define the two tunnel-end addresses.
- Configure a static route to the other FortiGate unit.

- Configure the tunnel network as part of the OSPF network and define the virtual IPsec interface as an OSPF interface.

This section describes the configuration with only one VPN, tunnel_wan1. The other VPN is added in the section OSPF over IPsec configuration on page 1750.

Configuring the IPsec VPN

A route-based VPN is required. In this chapter, preshared key authentication is shown. Certificate authentication is also possible. Both FortiGate units need this configuration.

To configure Phase 1

1. Define the Phase 1 configuration needed to establish a secure connection with the other FortiGate unit. For more information, see Phase 1 parameters on page 1581.

   Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel, tunnel_wan1 for example. This becomes the name of the virtual IPsec interface.
Remote Gateway	Select **Static IP Address**.
IP Address	Enter the IP address of the other FortiGate unit's public (Port 2) interface.
Local Interface	Select this FortiGate unit's public (Port 2) interface.
Mode	Select **Main (ID Protection)**.
Authentication Method	**Preshared Key**
Pre-shared Key	Enter the preshared key. It must match the preshared key on the other FortiGate unit.
Advanced	Select **Advanced**.

To assign the tunnel end IP addresses

1. Go to **System > Network > Interfaces**, select the virtual IPsec interface that you just created on Port 2 and select **Edit**.
2. In the **IP** and **Remote IP** fields, enter the following tunnel end addresses:

	FortiGate_1	FortiGate_2
IP	10.1.1.1	10.1.1.2
Remote_IP	10.1.1.2	10.1.1.1

These addresses are from a network that is not used for anything else.

To configure Phase 2

1. Enter a name to identify this Phase 2 configuration, twan1_p2, for example.
2. Select the name of the Phase 1 configuration that you defined in Step "OSPF over IPsec configuration" on page 1750, tunnel_wan1 for example.

Configuring static routing

You need to define the route for traffic leaving the external interface.

1. Go to **Router > Static > Static Route**s, select **Create New**.
   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the following information.

Destination IP/Mask	Leave as 0.0.0.0 0.0.0.0.
Device	Select the external interface.
Gateway	Enter the IP address of the next hop router.

Configuring OSPF

This section does not attempt to explain OSPF router configuration. It focusses on the integration of the IPsec tunnel into the OSPF network. This is accomplished by assigning the tunnel as an OSPF interface, creating an OSPF route to the other FortiGate unit.

This configuration uses loopback interfaces to ease OSPF troubleshooting. The OSPF router ID is set to the loopback interface address.The loopback interface ensures the router is always up. Even though technically the router ID doesn't have to match a valid IP address on the FortiGate unit, having an IP that matches the router ID makes troubleshooting a lot easier.

The two FortiGate units have slightly different configurations. FortiGate_1 is an AS border router that advertises its static default route. FortiGate_2 advertises its local LAN as an OSPF internal route.

Setting the router ID for each FortiGate unit to the lowest possible value is useful if you want the FortiGate units to be the designated router (DR) for their respective ASes. This is the router that broadcasts the updates for the AS.

Leaving the IP address on the OSPF interface at 0.0.0.0 indicates that all potential routes will be advertised, and it will not be limited to any specific subnet. For example if this IP address was 10.1.0.0, then only routes that match that subnet will be advertised through this interface in OSPF.

FortiGate_1 OSPF configuration

When configuring FortiGate_1 for OSPF, the loopback interface is created, and then you configure OSPF area networks and interfaces.

With the exception of creating the loopback interface, OSPF for this example can all be configured in either the web-based manager or CLI.

To create the loopback interface

A loopback interface can be configured in the CLI only. For example, if the interface will have an IP address of 10.0.0.1, you would enter:

```
config system interface
   edit lback1
      set vdom root
         set ip 10.0.0.1 255.255.255.255
         set type loopback
   end
```

The loopback addresses and corresponding router IDs on the two FortiGate units must be different. For example, set the FortiGate 1 loopback to 10.0.0.1 and the FortiGate 2 loopback to 10.0.0.2.

To configure OSPF area, networks, and interfaces - web-based manager

1. On FortiGate_1, go to **Router > Dynamic > OSPF**.
   For low end FortiGate units, you first need to enable **Dynamic Routing** by going to **System > Admin > Settings**.
2. Enter the following information to define the router, area, and interface information.

Router ID	Enter `10.0.0.1`. Select **Apply** before entering the remaining information.
Advanced Options	
Redistribute	Select the **Connected** and **Static** check boxes. Use their default metric values.
Areas	Select **Create New**, enter the **Area** and **Type** and then select **OK**.
Area	0.0.0.0
Type	Regular
Interfaces	Enter a name for the OSPF interface, ospf_wan1 for example.
Name	
Interface	Select the virtual IPsec interface, tunnel_wan1.
IP	0.0.0.0

3. For **Networks**, select **Create New**.
4. Enter the **IP/Netmask** of `10.1.1.0/255.255.255.0` and an **Area** of `0.0.0.0`.
5. For **Networks**, select **Create New**.
6. Enter the **IP/Netmask** of `10.0.0.1/255.255.255.0` and an **Area** of `0.0.0.0`.
7. Select **Apply**.

To configure OSPF area and interfaces - CLI

Your loopback interface is 10.0.0.1, your tunnel ends are on the 10.1.1.0/24 network, and your virtual IPsec interface is named `tunnel_wan1`. Enter the following CLI commands:

```
config router ospf
   set router-id 10.0.0.1
   config area
      edit 0.0.0.0
   end
   config network
      edit 4
         set prefix 10.1.1.0 255.255.255.0
      next
      edit 2
         set prefix 10.0.0.1 255.255.255.255
      end
   config ospf-interface
      edit ospf_wan1
         set cost 10
         set interface tunnel_wan1
         set network-type point-to-point
      end
   config redistribute connected
      set status enable
   end
   config redistribute static
      set status enable
   end
end
```

FortiGate_2 OSPF configuration

When configuring FortiGate_2 for OSPF, the loopback interface is created, and then you configure OSPF area networks and interfaces.

Configuring FortiGate_2 differs from FortiGate_1 in that three interfaces are defined instead of two. The third interface is the local LAN that will be advertised into OSPF.

With the exception of creating the loopback interface, OSPF for this example can all be configured in either the web-based manager or CLI.

To create the loopback interface

A loopback interface can be configured in the CLI only. For example, if the interface will have an IP address of 10.0.0.2, you would enter:

```
config system interface
   edit lback1
      set vdom root
      set ip 10.0.0.2 255.255.255.255
      set type loopback
   end
```

The loopback addresses on the two FortiGate units must be different. For example, set the FortiGate 1 loopback to 10.0.0.1 and the FortiGate 2 loopback to 10.0.0.2.

To configure OSPF area and interfaces - web-based manager

1. On FortiGate_2, go to **Router > Dynamic > OSPF**.

   For low end FortiGate units, you first need to enable **Dynamic Routing** by going to **System > Admin > Settings**.
2. Complete the following.

Router ID	10.0.0.2
Areas	Select **Create New**, enter the **Area** and **Type** and then select **OK**.
Area	0.0.0.0
Type	Regular
Interfaces	
Name	Enter a name for the OSPF interface, ospf_wan1 for example.
Interface	Select the virtual IPsec interface, tunnel_wan1.
IP	0.0.0.0

3. For **Networks**, select **Create New**.
4. Enter the following information for the loopback interface:

IP/Netmask	10.0.0.2/255.255.255.255
Area	0.0.0.0

5. For **Networks**, select **Create New**.
6. Enter the following information for the tunnel interface:

IP/Netmask	10.1.1.0/255.255.255.255
Area	0.0.0.0

7. For **Networks**, select **Create New**.
8. Enter the following information for the local LAN interface:

IP/Netmask	10.31.101.0/255.255.255.255
Area	0.0.0.0

9. Select **Apply**.

To configure OSPF area and interfaces - CLI

If for example, your loopback interface is 10.0.0.2, your tunnel ends are on the 10.1.1.0/24 network, your local LAN is 10.31.101.0/24, and your virtual IPsec interface is named tunnel_wan1, you would enter:

```
config router ospf
   set router-id 10.0.0.2
   config area
      edit 0.0.0.0
   end
   config network
      edit 1
         set prefix 10.1.1.0 255.255.255.0
      next
      edit 2
         set prefix 10.31.101.0 255.255.255.0
      next
      edit 2
         set prefix 10.0.0.2 255.255.255.255
      end
   config ospf-interface
      edit ospf_wan1
         set interface tunnel_wan1
         set network-type point-to-point
      end
end
```

Creating a redundant configuration

You can improve the reliability of the OSPF over IPsec configuration described in the previous section by adding a second IPsec tunnel to use if the default one goes down. Redundancy in this case is not controlled by the IPsec VPN configuration but by the OSPF routing protocol.

To do this you:

- Create a second route-based IPsec tunnel on a different interface and define tunnel end addresses for it.
- Add the tunnel network as part of the OSPF network and define the virtual IPsec interface as an additional OSPF interface.
- Set the OSPF cost for the added OSPF interface to be significantly higher than the cost of the default route.

Adding the second IPsec tunnel

The configuration is the same as in Creating a redundant configuration on page 1756, but the interface and addresses will be different. Ideally, the network interface you use is connected to a different Internet service provider for added redundancy.

When adding the second tunnel to the OSPF network, choose another unused subnet for the tunnel ends, 10.1.2.1 and 10.1.2.2 for example.

Adding the OSPF interface

OSPF uses the metric called cost when determining the best route, with lower costs being preferred. Up to now in this example, only the default cost of 10 has been used. Cost can be set only in the CLI.

The new IPsec tunnel will have its OSPF cost set higher than that of the default tunnel to ensure that it is only used if the first tunnel goes down. The new tunnel could be set to a cost of 200 compared to the default cost is 10. Such a large difference in cost will ensure this new tunnel will only be used as a last resort.

If the new tunnel is called tunnel_wan2, you would enter the following on both FortiGate units:

```
config router ospf
   config ospf-interface
      edit ospf_wan2
         set cost 200
         set interface tunnel_wan2
         set network-type point-to-point
      end
   end
```

Redundant OSPF routing over IPsec

This example sets up redundant secure communication between two remote networks using an Open Shortest Path First (OSPF) VPN connection. In this example, the HQ FortiGate unit will be called FortiGate 1 and the Branch FortiGate unit will be called FortiGate 2.

The steps include:

1. Creating redundant IPsec tunnels on FortiGate 1.
2. Configuring IP addresses and OSPF on FortiGate 1.
3. Configuring firewall addresses on FortiGate 1.
4. Configuring security policies on FortiGate 1.
5. Creating redundant IPsec tunnels for FortiGate 2.
6. Configuring IP addresses and OSPF on FortiGate 2.
7. Configuring firewall addresses on FortiGate 2.
8. Configuring security policies on FortiGate 2.

Creating redundant IPsec tunnels on FortiGate 1

1. Go to **VPN > IPsec > Tunnels**.
2. Select **Create New**, name the primary tunnel and select **Custom VPN Tunnel (No Template)**.
3. Set the following:

Remote Gateway	Static IP Address
IP Address	FortiGate 2's wan1 IP
Local Interface	wan1 (the primary Internet-facing interface)
Pre-shared Key	Enter

4. Go to **VPN > IPsec > Tunnels**.
5. Select **Create New**, name the secondary tunnel and select **Custom VPN Tunnel (No Template)**.
6. Set the following:

Remote Gateway	Static IP Address
IP Address	FortiGate 2's wan2 IP
Local Interface	wan2 (the secondary Internet-facing interface)
Pre-shared Key	Enter

Configuring IP addresses and OSPF on FortiGate 1

1. Go to **System > Network > Interfaces**.
2. Select the arrow for **wan1** to expand the list.

3. Edit the primary tunnel interface and create IP addresses.

IP	10.1.1.1
Remote IP	10.1.1.2

4. Select the arrow for **wan2** to expand the list.
5. Edit the secondary tunnel interface and create IP addresses.

IP	10.2.1.1
Remote IP	10.2.1.2

6. Go to **Router > Dynamic > OSPF** and enter the **Router ID** for FortiGate 1.
7. Select **Create New** in the **Area** section.
8. Add the backbone area of **0.0.0.0**.
9. Select **Create New** in the **Networks** section.
10. Create the networks and select **Area 0.0.0.0** for each one.
11. Select **Create New** in the **Interfaces** section.
12. Create primary and secondary tunnel interfaces.
13. Set a **Cost** of **10** for the primary interface and **100** for the secondary interface.

Configuring firewall addresses on FortiGate 1

1. Go to **Policy & Objects > Objects > Addresses**.
2. Create/Edit the subnets behind FortiGate 1 and FortiGate 2.
3. Create/Edit the primary and secondary interfaces of FortiGate 2.

Configuring security policies on FortiGate 1

1. Go to **Policy & Objects> Policy > IPv4**.
2. Create the four security policies required for both FortiGate 1's primary and secondary interfaces to connect to FortiGate 2's primary and secondary interfaces.

Creating redundant IPsec tunnels on FortiGate 2

1. Go to **VPN > IPsec > Tunnels**.
2. Select **Create New**, name the primary tunnel and select **Custom VPN Tunnel (No Template)**.
3. Set the following:

Remote Gateway	Static IP Address
IP Address	FortiGate 1's wan1 IP
Local Interface	wan1 (the primary Internet-facing interface)
Pre-shared Key	Enter

4. Go to **VPN > IPsec > Tunnels**.
5. Select **Create New**, name the secondary tunnel and select **Custom VPN Tunnel (No Template)**.
6. Set the following:

Remote Gateway	Static IP Address
IP Address	FortiGate 1's wan1 IP
Local Interface	wan2 (the secondary Internet-facing interface)
Pre-shared Key	Enter

Configuring IP addresses and OSPF on FortiGate 2

1. Go to **System > Network > Interfaces**.
2. Select the arrow for **wan1** to expand the list.
3. Edit the primary tunnel interface and create IP addresses.

IP	10.1.1.2
Remote IP	10.1.1.1

4. Select the arrow for **wan2** to expand the list.
5. Edit the secondary tunnel interface and create IP addresses.

IP	10.2.1.2
Remote IP	10.2.1.1

6. Go to **Router > Dynamic > OSPF** and enter the **Router ID** for FortiGate 2.
7. Select **Create New** in the **Area** section.
8. Add the backbone area of **0.0.0.0**.
9. Select **Create New** in the **Networks** section.
10. Create the networks and select **Area 0.0.0.0** for each one.
11. Select **Create New** in the **Interfaces** section.
12. Create primary and secondary tunnel interfaces.
13. Set a **Cost** of **10** for the primary interface and **100** for the secondary interface.

Configuring firewall addresses on FortiGate 2

1. Go to **Policy & Objects > Objects > Addresses**.
2. Create/Edit the subnets behind FortiGate 1 and FortiGate 2.
3. Create/Edit the primary and secondary interfaces of FortiGate 2.

Configuring security policies on FortiGate 2

1. Go to **Policy & Objects> Policy > IPv4**.
2. Create the four security policies required for both FortiGate 2's primary and secondary interfaces to connect to FortiGate 1's primary and secondary interfaces.

Results

1. Go to **VPN > Monitor > IPsec Monitor** to verify the statuses of both the primary and secondary IPsec VPN tunnels on FortiGate 1 and FortiGate 2.
2. Go to **Router > Monitor > Routing**. Monitor to verify the routing table on FortiGate 1 and FortiGate 2. Type **OSPF** for the **Type** and select **Apply Filter** to verify the OSPF route.
3. Verify that traffic flows via the primary tunnel:
   - From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a tracert to a PC2 set to IP address 10.21.1.00 behind FortiGate 2 and vise versa.
   - From PC1, you should see that the traffic goes through 10.1.1.2 which is the primary tunnel interface IP set on FortiGate 2.
   - From PC2, you should see the traffic goes through 10.1.1.1 which is the primary tunnel interface IP set on FortiGate 1.
4. The VPN network between the two OSPF networks uses the primary VPN connection. Disconnect the wan1 interface and confirm that the secondary tunnel will be used automatically to maintain a secure connection.
5. Verify the IPsec VPN tunnel statuses on FortiGate 1 and FortiGate 2. Both FortiGates should show that primary tunnel is DOWN and secondary tunnel is UP.
6. Go to **VPN > Monitor > IPsec Monitor** to verify the status.
7. Verify the routing table on FortiGate 1 and FortiGate 2.
   The secondary OSPF route (with cost = 100) appears on both FortiGate units.
8. Go to **Router > Monitor > Routing Monitor**. Type **OSPF** for the **Type** and select **Apply Filter** to verify OSPF route.
9. Verify that traffic flows via the secondary tunnel:
   - From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a tracert to a PC2 set to IP:10.21.1.100 behind FortiGate 2 and vice versa.
   - From PC1, you should see that the traffic goes through 10.2.1.2 which is the secondary tunnel interface IP set on FortiGate 2.
   - From PC2, you should see the traffic goes through 10.2.1.1 which is the secondary tunnel interface IP set on FortiGate 1.

OSPF over dynamic IPsec

This example shows how to create a dynamic IPsec VPN tunnel that allows OSPF.

Configuring IPsec on FortiGate 1

1. Go to **System > Status** and enter the **CLI Console** widget
2. Create phase 1:

```
config vpn ipsec phase1-interface
   edit "dial-up"
      set type dynamic
      set interface "wan1"
      set mode-cfg enable
      set proposal 3des-sha1
      set add-route disable
      set ipv4-start-ip 10.10.101.0
      set ipv4-end-ip 10.10.101.255
      set psksecret
   next
end
```

3. Create phase 2:

```
config vpn ipsec phase2-interface
   edit "dial-up-p2"
      set phase1name "dial-up"
      set proposal 3des-sha1 aes128-sha1
   next
end
```

Configuring OSPF on FortiGate 1

1. Go to **System > Status** and enter the **CLI Console** widget.
2. Create OSPF route.

```
config router ospf
   set router-id 172.20.120.22
      config area
         edit 0.0.0.0
         next
      end
      config network
         edit 1
            set prefix 10.10.101.0 255.255.255.0
         next
      end
      config redistribute "connected"
         set status enable
      end
      config redistribute "static"
         set status enable
      end
end
```

Adding policies on FortiGate 1

1. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from **dial-up** to **port5**.
2. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from **port5** to **dial-up** interfaces.

Configuring IPsec on FortiGate 2

1. Go to **System > Status** and enter the **CLI Console** widget
2. Create phase 1:

```
config vpn ipsec phase1-interface
   edit "dial-up-client"
      set interface "wan1"
      set mode-cfg enable
      set proposal 3des-sha1
      set add-route disable
      set remote-gw 172.20.120.22
      set psksecret
   next
end
```

3. Create phase 2:

```
config vpn ipsec phase2-interface
   edit "dial-up-client"
      set phase1name "dial-up-client"
      set proposal 3des-sha1 aes128-sha1
      set auto-negotiate enable
   next
end
```

Configuring OSPF on FortiGate 2

1. Go to **System > Status** and enter the **CLI Console** widget.
2. Create OSPF route.

```
config router ospf
   set router-id 172.20.120.15
      config area
         edit 0.0.0.0
         next
      end
      config network
         edit 1
            set prefix 10.10.101.0 255.255.255.0
         next
      end
      config redistribute "connected"
         set status enable
      end
      config redistribute "static"
         set status enable
      end
end
```

Adding policies on FortiGate 2

1. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from **dial-up-client** to **port5**.
2. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from **port5** to **dial-up-client** interfaces.

Verifying the tunnel is up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **Up**.

Results

1. From FortiGate 1, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via OSPF.
2. From FortiGate 1, go to **System > Status**. Enter the CLI Console widget and type this command to verify OSPF neighbors:
   ```
   get router info ospf neighbor
   ```
3. From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via OSPF.
4. From FortiGate 2, go to **System > Status**. Enter the CLI Console widget and type this command to verify OSPF neighbors:
   ```
   get router info ospf neighbor
   ```

BGP over dynamic IPsec

This example shows how to create a dynamic IPsec VPN tunnel that allows BGP.

Configuring IPsec on FortiGate 1

1. Go to **Policy & Objects > Objects > Addresses** and select create new **Address**.

Name	Remote_loop_int
Type	Subnet
Subnet/IP Range	10.10.10.10
Interface	any

2. Create an **Address Group**.

Group Name	VPN_DST
Show in Address List	enable
Members	Remote_loop_int all

3. Go to **System > Status** and enter the CLI Console widget.
4. Create phase 1:

```
config vpn ipsec phase1-interface
   edit Dialup
      set type dynamic
      set interface wan1
      set mode aggressive
      set peertype one
      set mode-cfg enable
      set proposal 3des-sha1 aes128-sha1
      set peerid dial
      set assign-ip disable
      set psksecret
   next
end
```

5. Create phase 2:

```
config vpn ipsec phase2-interface
   edit dial_p2
      set phase1name Dialup
      set proposal 3des-sha1 aes128-sha1
      set src-addr-type name
      set dst-addr-type name
      set src-name all
      set dst-name VPN_DST
   next
```

```
end
```

Configuring BGP on FortiGate 1

1. Go to **System > Network > Interfaces** and create a Loopback interface.
2. Set **IP/Network Mask** to **20.20.20.20/255.255.255.255**.
3. Go to **System > Status** and enter the CLI Console widget.
4. Create a BGP route.

```
config router bgp
   set as 100
   set router-id 1.1.1.1
      config neighbor
         edit 10.10.10.10
            set ebgp-enforce-multihop enable
            set remote-as 200
            set update-source loop
         next
      end
      config redistribute connected
         set status enable
      end
end
```

Adding policies on FortiGate 1

1. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.
2. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

Configuring IPsec on FortiGate 2

1. Go to **System > Status** and enter the CLI Console widget.
2. Create phase 1:

```
config vpn ipsec phase1-interface
   edit Dialup
      set interface wan1
      set mode aggressive
      set mode-cfg enable
      set proposal 3des-sha1 aes128-sha1
      set localid dial
      set remote-gw 172.20.120.22
      set assign-ip disable
      set psksecret
   next
end
```

3. Create phase 2:

```
config vpn ipsec phase2-interface
   edit dial_p2
      set phase1name Dialup
      set proposal 3des-sha1 aes128-sha1
      set keepalive enable
```

```
    next
end
```

Configuring BGP on FortiGate 2

1. Go to **System > Network > Interfaces** and create a Loopback interface.
2. Set **IP/Network Mask** to **10.10.10.10/255.255.255.255**.
3. Go to **System > Status** and enter the **CLI Console** widget.
4. Create a BGP route.

```
config router bgp
   set as 200
   set router-id 1.1.1.2
      config neighbor
         edit 20.20.20.20
            set ebgp-enforce-multihop enable
            set remote-as 100
            set update-source loop
         next
      end
      config redistribute connected
         set status enable
      end
end
```

Adding policies on FortiGate 2

1. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.
2. Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

Adding a static route on FortiGate 2

Go to **Router > Static > Static Routes** and add a route to the remote Loopback interface via Dialup interface.

Destination IP/Mask	20.20.20.20/255.255.255.255
Device	Dialup
Administrative Distance	10

Verifying the tunnel is up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **Up**.

Results

1. From FortiGate 1, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via BGP.

2. From FortiGate 1, go to **System > Status**.
3. Enter the **CLI Console** widget and type this command to verify BGP neighbors:
```
get router info bgp summary
```
4. From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via BGP.
5. From FortiGate 2, go to **System > Status**.
6. Enter the **CLI Console** widget and type this command to verify BGP neighbors:
```
get router info bgp summary
```

Logging and monitoring

This section provides some general logging and monitoring procedures for VPNs.

The following topics are included in this section:

Monitoring VPN connections
Logging VPN events

Monitoring VPN connections

You can use the monitor to view activity on IPsec VPN tunnels and to start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels.

Monitoring connections to remote peers

The list of tunnels provides information about VPN connections to remote peers that have static IP addresses or domain names. You can use this list to view status and IP addressing information for each tunnel configuration. You can also start and stop individual tunnels from the list.

To view the list of static-IP and dynamic-DNS tunnels go to **VPN > Monitor > IPsec Monitor**.

Monitoring dialup IPsec connections

The list of dialup tunnels provides information about the status of tunnels that have been established for dialup clients. The list displays the IP addresses of dialup clients and the names of all active tunnels. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

To view the list of dialup tunnels go to **VPN > Monitor > IPsec Monitor**.

If you take down an active tunnel while a dialup client such as FortiClient is still connected, FortiClient will continue to show the tunnel connected and idle. The dialup client must disconnect before another tunnel can be initiated.

The list of dialup tunnels displays the following statistics:

- The Name column displays the name of the tunnel.
- The meaning of the value in the Remote gateway column changes, depending on the configuration of the network at the far end:
  - When a FortiClient dialup client establishes a tunnel, the Remote gateway column displays either the public IP address and UDP port of the remote host device (on which the FortiClient Endpoint Security application is installed), or if a NAT device exists in front of the remote host, the Remote gateway column displays the public IP address and UDP port of the remote host.
  - When a FortiGate dialup client establishes a tunnel, the Remote gateway column displays the public IP address and UDP port of the FortiGate dialup client.
- The Username column displays the peer ID, certificate name, or XAuth user name of the dialup client (if a peer ID, certificate name, or XAuth user name was assigned to the dialup client for authentication purposes).
- The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

- The Proxy ID Source column displays the IP addresses of the hosts, servers, or private networks behind the FortiGate unit. A network range may be displayed if the source address in the security encryption policy was expressed as a range of IP addresses.
- The meaning of the value in the Proxy ID Destination column changes, depending on the configuration of the network at the far end:
  - When a FortiClient dialup client establishes a tunnel:
  - If VIP addresses are not used and the remote host connects to the Internet directly, the Proxy ID Destination field displays the public IP address of the Network Interface Card (NIC) in the remote host.
  - If VIP addresses are not used and the remote host is behind a NAT device, the Proxy ID Destination field displays the private IP address of the NIC in the remote host.
  - If VIP addresses were configured (manually or through FortiGate DHCP relay), the Proxy ID Destination field displays either the VIP address belonging to a FortiClient dialup client, or a subnet address from which VIP addresses were assigned.
- When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.

Logging VPN events

You can configure the FortiGate unit to log VPN events. For IPsec VPNs, Phase 1 and Phase 2 authentication and encryption events are logged. For information about how to interpret log messages, see the FortiGate Log Message Reference.

To log VPN events

1. Go to **Log & Report > Log Config > Log Settings**.
2. Verify that the **VPN activity event** option is selected.
3. Select **Apply**.

To view event logs

1. Go to **Log & Report > Event Log > VPN**.
2. Select the **Log location**.

Sending tunnel statistics to FortiAnalyzer

By default, logged events include tunnel-up and tunnel-down status events. Other events, by default, will appear in the FortiAnalyzer report as "No Data Available". More accurate results require logs with `action=tunnel-stats`, which is used in generating reports on the FortiAnalyzer (rather than the tunnel-up and tunnel-down event logs). The FortiGate does not, by default, send `tunnel-stats` information.

To allow VPN `tunnel-stats` to be sent to FortiAnalyzer, configure the FortiGate unit as follows using the CLI:

```
config system settings
   set vpn-stats-log ipsec ssl
   set vpn-stats-period 300
end
```

Troubleshooting

This section contains tips to help you with some common challenges of IPsec VPNs.

A VPN connection has multiple stages that can be confirmed to ensure the connection is working properly. It is easiest to see if the final stage is successful first since if it is successful the other stages will be working properly. Otherwise, you will need to work back through the stages to see where the problem is located.

When a VPN connection is properly established, traffic will flow from one end to the other as if both ends were physically in the same place. If you can determine the connection is working properly then any problems are likely problems with your applications.

On some FortiGate units, such as the FortiGate 94D, you cannot ping over the IPsec tunnel without first setting a source-IP. In this scenario, you must assign an IP address to the virtual IPSEC VPN interface. Anything sourced from the FortiGate going over the VPN will use this IP address.

If the egress/outgoing interface (determined by kernel route) has an IP address, then use the IP address of the egress/outgoing interface. Otherwise, use the IP address of the first interface from the interface list (that has an IP address).

The first diagnostic command worth running, in any IPsec VPN troubleshooting situation, is the following:

```
diagnose vpn tunnel list
```

This command is very useful for gathering statistical data such as the number of packets encrypted versus decrypted, the number of bytes sent versus received, the SPI identifier, etc. This kind of information in the resulting output can make all the difference in determining the issue with the VPN.

Another appropriate diagnostic command worth trying is:

```
diagnose debug flow
```

This command will inform you of any lack of firewall policy, lack of forwarding route, and of policy ordering issues.

The following is a list of such potential issues. Bear in mind that the troubleshooting suggestions below are not exhaustive, and may not reflect your network topology.

The options to configure policy-based IPsec VPN are unavailable.

Go to **System > Config > Features**. Select **Show More** and turn on **Policy-based IPsec VPN**.

The VPN connection attempt fails.

If your VPN fails to connect, check the following:

- Ensure that the **pre-shared keys** match exactly (see The pre-shared key does not match (PSK mismatch error). below).
- Ensure that both ends use the same P1 and P2 proposal settings (seeThe SA proposals do not match (SA proposal mismatch). below).
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.

- Ensure that your FortiGate unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy. You might need to pin the PAT/NAT session table, or use some of kind of NAT-T keepalive to avoid the expiration of your PAT/NAT translation.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly on the
- FortiGate and that clients have specified the correct Local ID.
- If you are using FortiClient, ensure that your version is compatible with the FortiGate firmware by reading the FortiOS Release Notes.
- If you are using Perfect Forward Secrecy (PFS), ensure that it is used on both peers. You can use the `diagnose vpn tunnel list` command to troubleshoot this.
- Ensure that the **Quick Mode selectors** are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range. This is especially useful if the remote endpoint is not a FortiGate device.
- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the FortiGate unit is set to **Enable as Server**.
- Check IPsec VPN Maximum Transmission Unit (MTU) size. A 1500 byte MTU is going to exceed the overhead of the ESP-header, including the additional ip_header,etc. You can use the `diagnose vpn tunnel list` command to troubleshoot this.
- If your FortiGate unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your FortiGate unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the following diagnostic command in the CLI:

```
diagnose debug application ike -1
diagnose debug enable
```

The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

```
diagnose debug reset
diagnose debug disable
```

The VPN tunnel goes down frequently.

If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.

The pre-shared key does not match (PSK mismatch error).

It is possible to identify a PSK mismatch using the following combination of CLI commands:

```
diag debug app ike filter name "phase1-name"
diag debug app ike -1
diag debug enable
```

This will provide you with clues as to any PSK or other proposal issues. If it is a PSK mismatch, you should see something similar to the following output:

```
ike 0:TRX:322: PSK auth failed: probable pre-shared key mismatch
ike Negotiate SA Error:
```

The SA proposals do not match (SA proposal mismatch).

The most common problem with IPsec VPN tunnels is a mismatch between the proposals offered between each party. Without a match and proposal agreement, Phase 1 can never establish. Use the following command to show the proposals presented by both parties.

```
diag debug app ike -1
diag debug enable
```

The resulting output should include something similar to the following, where blue represents the remote VPN device, and green represents the local FortiGate.

```
responder received SA_INIT msg
incoming proposal:
proposal id = 1:
   protocol = IKEv2:
      encapsulation = IKEv2/none
         type=ENCR, val=AES_CBC (key_len = 256)
         type=INTEGR, val=AUTH_HMAC_SHA_96
         type=PRF, val=PRF_HMAC_SHA
         type=DH_GROUP, val=1536.
proposal id = 2:
   protocol = IKEv2:
      encapsulation = IKEv2/none
         type=ENCR, val=3DES_CBC
         type=INTEGR, val=AUTH_HMAC_SHA_2_256_128
         type=PRF, val=PRF_HMAC_SHA2_256
         type=DH_GROUP, val=1536.
proposal id = 1:
   protocol = IKEv2:
      encapsulation = IKEv2/none
         type=ENCR, val=AES_CBC (key_len = 128)
         type=INTEGR, val=AUTH_HMAC_SHA_96
         type=PRF, val=PRF_HMAC_SHA
         type=DH_GROUP, val=1536.
```

Pre-existing IPsec VPN tunnels need to be cleared.

Should you need to clear an IKE gateway, use the following commands:

```
diagnose vpn ike restart
diagnose vpn ike gateway clear
```

LAN interface connection

To confirm whether a VPN connection over LAN interfaces has been configured correctly, issue a ping or traceroute command on the network behind the FortiGate unit to test the connection to a computer on the remote network. If the connection is properly configured, a VPN tunnel will be established automatically when the first data packet destined for the remote network is intercepted by the FortiGate unit.

If the ping or traceroute fail, it indicates a connection problem between the two ends of the tunnel. This may or may not indicate problems with the VPN tunnel. You can confirm this by going to **VPN > Monitor > IPsec**

Monitor where you will be able to see your connection. A green arrow means the tunnel is up and currently processing traffic. A red arrow means the tunnel is not processing traffic, and this VPN connection has a problem.

If the connection has problems, see Troubleshooting VPN connections on page 1774.

Dialup connection

A dialup VPN connection has additional steps. To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

If the ping or traceroute fail, it indicates a connection problem between the two ends of the tunnel. This may or may not indicate problems with the VPN tunnel, or dialup client. As with the LAN connection, confirm the VPN tunnel is established by checking **VPN > Monitor > IPsec Monitor**.

Troubleshooting VPN connections

If you have determined that your VPN connection is not working properly through Troubleshooting on page 1771, the next step is to verify that you have a phase2 connection.

If traffic is not passing through the FortiGate unit as you expect, ensure the traffic does not contain IPcomp packets (IP protocol 108, RFC 3173). FortiGate units do not allow IPcomp packets, they compress packet payload, preventing it from being scanned.

Testing Phase 1 and 2 connections is a bit more difficult than testing the working VPN. This is because they require diagnose CLI commands. These commands are typically used by Fortinet customer support to discover more information about your FortiGate unit and its current configuration.

Before you begin troubleshooting, you must:

- Configure FortiGate units on both ends for interface VPN
- Record the information in your VPN Phase 1 and Phase 2 configurations - for our example here the remote IP address is 10.11.101.10 and the names of the phases are Phase 1 and Phase 2
- Install a telnet or SSH client such as putty that allows logging of output
- Ensure that the admin interface supports your chosen connection protocol so you can connect to your FortiGate unit admin interface.

For this example, default values were used unless stated otherwise.

To get diagnose information for the VPN connection - CLI

1. Log into the CLI as admin with the output being logged to a file.
2. Stop any diagnose debug sessions that are currently running with the CLI command
   ```
   diagnose debug disable
   ```
3. Clear any existing log-filters by running
   ```
   diagnose vpn ike log-filter clear
   ```
4. Set the log-filter to the IP address of the remote computer (10.11.101.10). This filters out all VPN connections except ones to the IP address we are concerned with. The command is
   ```
   diagnose vpn ike log-filter dst-addr4 10.11.101.10.
   ```
5. Set up the commands to output the VPN handshaking. The commands are:
   ```
   diagnose debug app ike 255
   ```

```
diagnose debug enable
```

6. Have the remote FortiGate initiate the VPN connection in the web-based manager by going to **VPN > Monitor** and selecting **Bring up**.

   This makes the remote FortiGate the initiator and the local FortiGate becomes the responder. Establishing the connection in this manner means the local FortiGate will have its configuration information as well as the information the remote computer sends. Having both sets of information locally makes it easier to troubleshoot your VPN connection.
7. Watch the screen for output, and after roughly 15 seconds enter the following CLI command to stop the output.
   ```
   diagnose debug disable
   ```
8. If needed, save the log file of this output to a file on your local computer. Saving the output to a file can make it easier to search for a particular phrase, and is useful for comparisons.

To troubleshoot a phase1 VPN connection

Using the output from To get diagnose information for the VPN connection - CLI on page 1774, search for the word `proposal` in the output. It may occur once indicating a successful connection, or it will occur two or more times for an unsuccessful connection — there will be one proposal listed for each end of the tunnel and each possible combination in their settings. For example if 10.11.101.10 selected both Diffie-Hellman Groups 1 and 5, that would be at least 2 proposals set.

A successful negotiation proposal will look similar to

```
IPsec SA connect 26 10.12.101.10->10.11.101.10:500
config found
created connection: 0x2f55860 26 10.12.101.10->10.11.101.10:500
IPsec SA connect 26 10.12.101.10->10.11.101.10:500 negotiating
no suitable ISAKMP SA, queuing quick-mode request and initiating ISAKMP SA negotiation
initiator: main mode is sending 1st message...
cookie 3db6afe559e3df0f/0000000000000000
out [encryption]
sent IKE msg (ident-i1send): 10.12.101.10:500->10.11.101.10:500, len=264,
    id=3db6afe559e3df0f/0000000000000000
diaike 0: comes 10.12.101.1:500->10.11.101.1:500,ifindex=26....
```

Note the phrase "`initiator: main mode is sending 1st message...`" which shows you the handshake between the ends of the tunnel is in progress. Initiator shows the remote unit is sending the first message.

VPN troubleshooting tips

More in-depth VPN troubleshooting can be found in the Troubleshooting guide.

Attempting hardware offloading beyond SHA1

If you are trying to off-load VPN processing to a network processing unit (NPU), remember that only SHA1 authentication is supported. For high levels of authentication such as SHA256, SHA384, and SHA512 hardware offloading is not an option — all VPN processing must be done in software.

Check Phase 1 proposal settings

Ensure that both sides have at least one Phase 1 proposal in common. Otherwise they will not connect. If there are many proposals in the list, this will slow down the negotiating of Phase 1. If its too slow, the connection may timeout before completing. If this happens, try removing some of the unused proposals.

NPU offloading is supported when the local gateway is a loopback interface.

Check your routing

If routing is not properly configured with an entry for the remote end of the VPN tunnel, traffic will not flow properly. You may need static routes on both ends of the tunnel. If routing is the problem, the proposal will likely setup properly but no traffic will flow.

Try enabling XAuth

If one end of an attempted VPN tunnel is using XAuth and the other end is not, the connection attempt will fail. The log messages for the attempted connection will not mention XAuth is the reason, but when connections are failing it is a good idea to ensure both ends have the same XAuth settings. If you do not know the other end's settings enable or disable XAuth on your end to see if that is the problem.

General troubleshooting tips

Most connection failures are due to a configuration mismatch between the FortiGate unit and the remote peer. In general, begin troubleshooting an IPsec VPN connection failure as follows:

1. Ping the remote network or client to verify whether the connection is up. See General troubleshooting tips on page 1776.
2. Traceroute the remote network or client. If DNS is working, you can use domain names. Otherwise use IP addresses.
3. Check the routing behind the dialup client. Routing problems may be affecting DHCP. If this appears to be the case, configure a DHCP relay service to enable DHCP requests to be relayed to a DHCP server on or behind the FortiGate server.
4. Verify the configuration of the FortiGate unit and the remote peer. Check the following IPsec parameters:
   - The mode setting for ID protection (main or aggressive) on both VPN peers must be identical.
   - The authentication method (preshared keys or certificates) used by the client must be supported on the FortiGate unit and configured properly.
   - If preshared keys are being used for authentication purposes, both VPN peers must have identical preshared keys.
   - The remote client must have at least one set of Phase 1 encryption, authentication, and Diffie-Hellman settings that match corresponding settings on the FortiGate unit.
   - Both VPN peers must have the same NAT traversal setting (enabled or disabled).
   - The remote client must have at least one set of Phase 2 encryption and authentication algorithm settings that match the corresponding settings on the FortiGate unit.
   - If you are using manual keys to establish a tunnel, the **Remote SPI** setting on the FortiGate unit must be identical to the **Local SPI** setting on the remote peer, and vise versa.
5. To correct the problem, see the following table.

VPN trouble-shooting tips

Configuration problem	Correction
Mode settings do not match.	Select complementary mode settings. See Phase 1 parameters on page 1581.
Peer ID or certificate name of the remote peer or dialup client is not recognized by FortiGate VPN server.	Check Phase 1 configuration. Depending on the Remote Gateway and Authentication Method settings, you have a choice of options to authenticate FortiGate dialup clients or VPN peers by ID or certificate name (see Phase 1 parameters on page 1581). If you are configuring authentication parameters for FortiClient dialup clients, refer to the Authenticating FortiClient Dialup Clients Technical Note.
Preshared keys do not match.	Reenter the preshared key. See Phase 1 parameters on page 1581.
Phase 1 or Phase 2 key exchange proposals are mismatched.	Make sure that both VPN peers have at least one set of proposals in common for each phase. See Phase 1 parameters on page 1581 and Phase 2 parameters on page 1598.
NAT traversal settings are mismatched.	Select or clear both options as required. See Phase 1 parameters on page 1581 and Phase 1 parameters on page 1581.

A word about NAT devices

When a device with NAT capabilities is located between two VPN peers or a VPN peer and a dialup client, that device must be NAT traversal (NAT-T) compatible for encrypted traffic to pass through the NAT device. For more information, see Phase 1 parameters on page 1581.

Chapter 15 - IPv6

The origins of Internet Protocol Version 6 (IPv6) date back to December 1998 with the publication of RFC 2460, which describes IPv6 as the successor to IPv4, the standard communications protocol still in use by the majority of users today. This transition away from IPv4 was a direct response to the foreseeable exhaustion of 32-bit IPv4 addresses, which are virtually all but assigned—all 4.3 billion.

IPv4 uses 32-bit addresses, which means that there is a theoretical address limit of 2 to the power of 32. The IPv6 address scheme is based on a 128-bit address, resulting in a theoretical address limit of 2 to the power of 128.

Possible addresses:

IPv4 = Roughly 4.3 billion

IPv6 = Over 340 undecillion (340 followed by 36 digits)

Assuming a world population of approximately 8 billion people, IPv6 would allow for each individual to have approximately 42,535,295,865,117,200,000,
000,000,000 devices with an IP address. That's 42 quintillion devices, so it's unlikely that we will ever need to worry about the availability of IPv6 addresses.

Aside from the difference of possible addresses, there is also the different formatting of the addresses. A computer would view an IPv4 address as a 32-bit string of binary digits made up of 1s and 0s, broken up into 4 octets of 8 digits separated by a period:

```
10101100.00010000.11111110.00000001
```

To make the number more user-friendly, we translate the address into decimal, again 4 octets separated by a period:

```
172.16.254.1
```

A computer would view an IPv6 address as a 128-bit string of binary digits made up of 1s and 0s, broken up into 8 octets of 16 digits separated by a colon:

```
0010000000000001:0000110110111:0000000000000000:0000000000010:0000000000000000:0000000000000000:0000000000000000:0000000000100000
```

To make this number a little more user-friendly, we translate it into hexadecimal, again 8 octets separated by a colon, for example:

```
2001:0db8:0000:0002:0000:0000:0000:0020
```

We can further simplify the above address. Because any four-digit group of zeros within an IPv6 address may be reduced to a single zero or altogether omitted, the above address can be reduced to:

```
2001:0db8:0000:0002:0:0:0:20
```

or

```
2001:db8:0:2::20
```

IPv6 packet structure

Each IPv6 packet consists of a mandatory fixed header and optional extension headers, and carries a payload, which is typically either a datagram and/or Transport Layer information. The payload could also contain data for the Internet Layer or Link Layer. Unlike IPv4, IPv6 packets aren't fragmented by routers, requiring hosts to implement Maximum Transmission Unit (MTU) Path Discovery for MTUs larger than the smallest MTU (which is 1280 octets).

Jumbograms and jumbo payloads

In IPv6, packets which exceed the MTU of the underlying network are labelled jumbograms, which consist of a jumbo payload. A jumbogram typically exceeds the IP MTU size limit of 65,535 octets, and provides the jumbo payload option, which can allow up to nearly 4GiB of payload data, as defined in RFC 2675. When the MTU is determined to be too large, the receiving host sends a 'Packet too Big' ICMPv6 type 2 message to the sender.

Fragmentation and reassembly

As noted, packets that are too large for the MTU require hosts to perform MTU Path Discovery to determine the maximum size of packets to send. Packets that are too large require a 'Fragment' extension header, to divide the payload into segments that are 8 octets in length (except for the last fragment, which is smaller). Packets are reassembled according to the extension header and the fragment offset.

Benefits of IPv6

Some of the benefits of IPv6 include:

- More efficient routing
- Reduced management requirement
- Stateless auto-reconfiguration of hosts
- Improved methods to change Internet Service Providers
- Better mobility support
- Multi-homing
- Security
- Scoped address: link-local, site-local, and global address space

IPv6 Features

In order to configure IPv6 features using the web-based manager, IPv6 must be enabled using Feature Select. Go to **System > Config > Features**, enable IPv6, and click **Apply**.

The following IPv6 features are available from the FortiOS web manager:

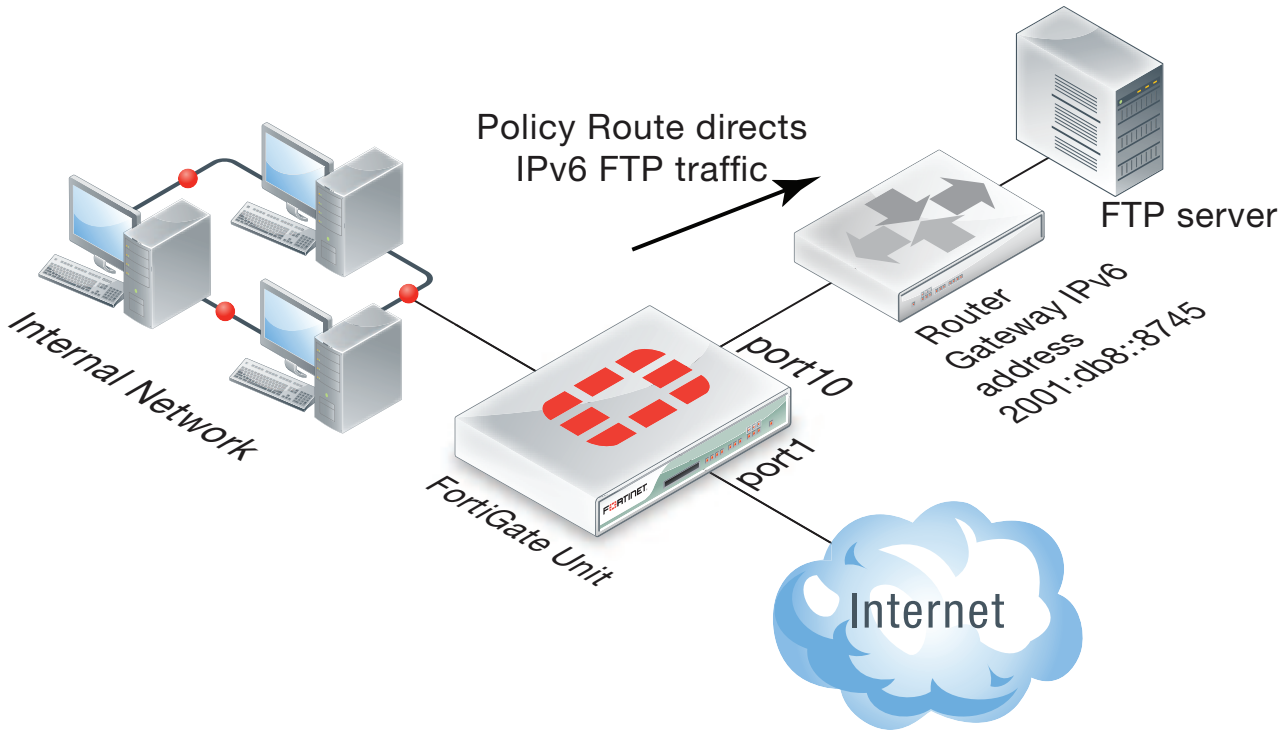
IPv6 policies
IPv6 Network Address Translation
ICMPv6
IPv6 in dynamic routing
Dual stack routing
IPv6 tunnelling
SIP over IPv6
New Fortinet FortiGate IPv6 MIB fields
IPv6 Per-IP traffic shaper
DHCPv6
IPv6 forwarding
Obtaining IPv6 addresses from an IPv6 DHCP server

IPv6 policies

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6 but must still have access to the Internet or must connect over an IPv4 network.

These policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks. The IPv6 options for creating these policies is hidden by default. You must enable this feature under **System > Config > Features**.

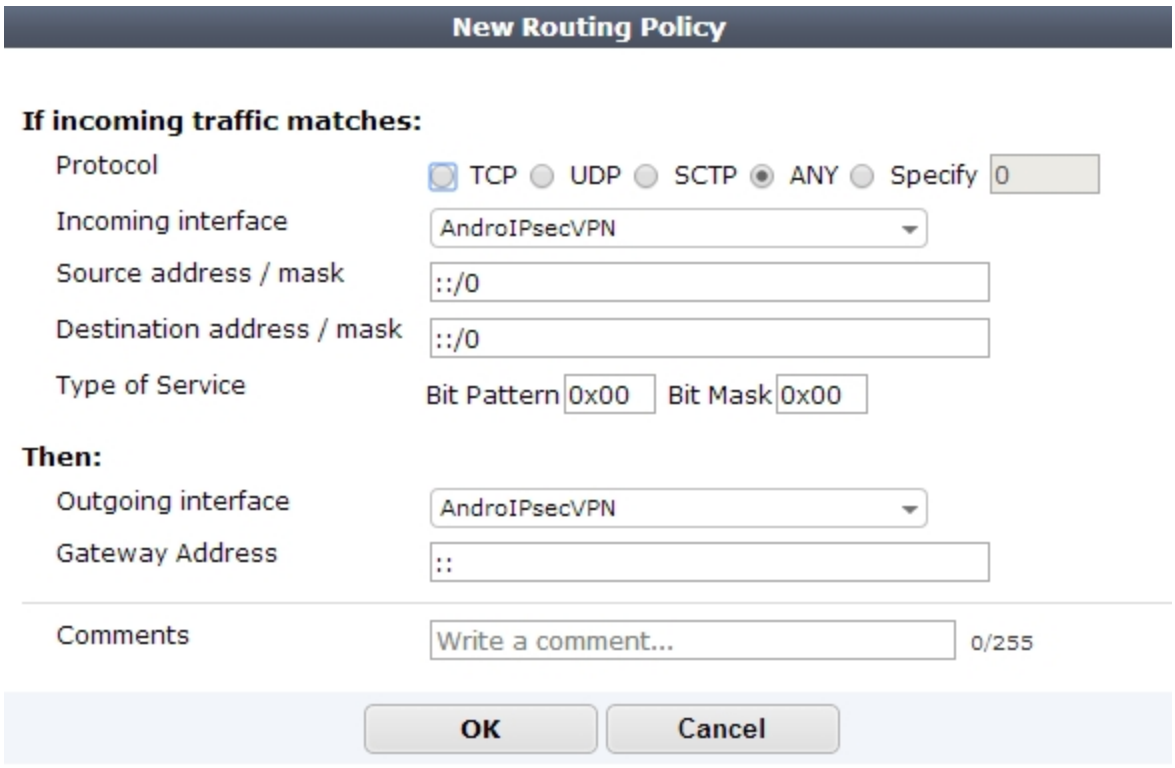
IPv6 policy route



IPv6 policy routing

IPv6 policy routing functions in the same was as IPv4 policy routing. To add an IPv6 policy route, go to **Router > Static > Policy Routes** and select **Create New > IPv6 Policy Route**.

Adding an IPv6 Policy route



You can also use the following command to add IPv6 policy routes:

```
config router policy6
   edit 0
      set input-device <interface>
      set src <ipv6_ip>
      set dst <ipv6_ip>
      set protocol <0-255>
      set gateway <ipv6_ip>
      set output-device <interface>
      set tos <bit_pattern>
      set tos-mask <bit_mask>
   end
```

IPv6 security policies

IPv6 security policies support all the features supported by IPv4 security policies:

- Policy types and subtypes.
- NAT support including using the destination interface IP address, fixed port, and dynamic IP pools.
- All security features (antivirus, web filtering, application control, IPS, email filtering, DLP, VoIP, and ICAP).
- All traffic shaping options, including: shared traffic shaping, reverse shared traffic shaping, and per-IP traffic shaping.
- All user and device authentication options.

IPv6 Policy Monitor

Once policies have been configured and enabled it is useful to be able to monitor them. To get an overview about what sort of traffic the policies are processing, go to **Policy & Objects > Monitor > IPv6 Policy Monitor**.

IPv6 explicit web proxy

You can use the explicit web proxy for IPv6 traffic. To do this you need to:

- Enable the Explicit Proxy from the dashboard.
- Enable the IPv6 explicit web proxy from the CLI.
- Enable the explicit web proxy for one or more FortiGate interfaces. These interfaces also need IPv6 addresses.
- Add IPv6 web proxy security policies to allow the explicit web proxy to accept IPv6 traffic.

Use the following steps to set up a FortiGate unit to accept IPv6 traffic for the explicit web proxy at the Internal interface and forward IPv6 explicit proxy traffic out the wan1 interface to the Internet.

1. Go to **System > Dashboard > Status** and turn on **Explicit Proxy** under the **Features > Security Features** widget. Click **Apply**.
2. Enter the following CLI command to enable the IPv6 explicit web proxy:

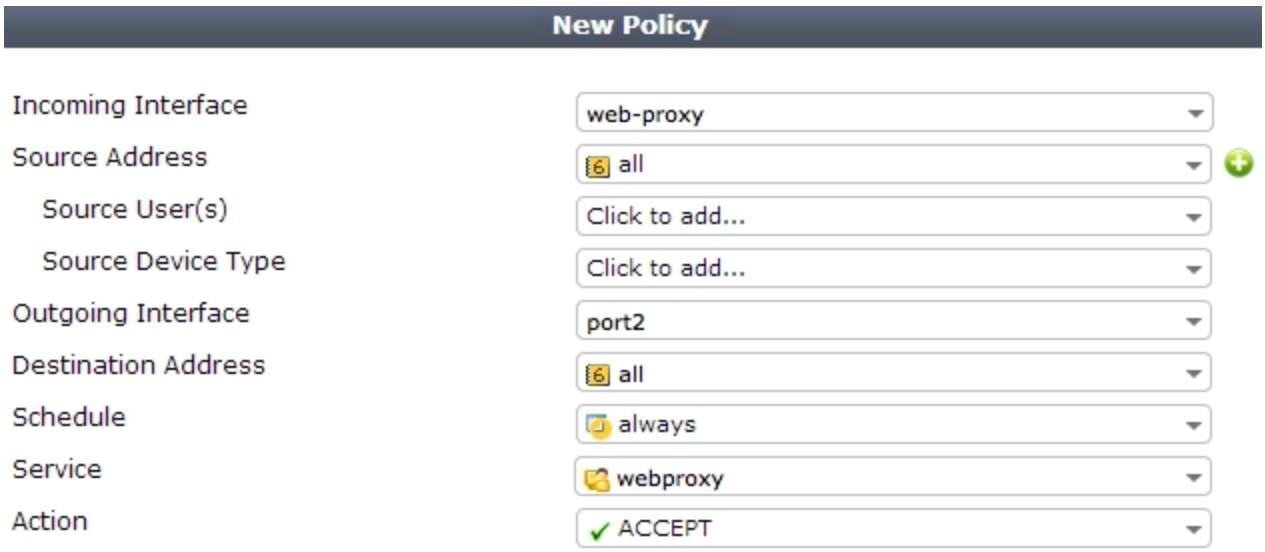
```
config web-proxy explicit
   set status enable
   set ipv6-status enable
end
```

3. Go to **System > Network > Interfaces** and edit the **internal** interface, select **Enable Explicit Web Proxy** and select **OK**.
4. Go to **Policy & Objects > Policy > IPv6** and select **Create New** to add an IPv6 explicit web proxy security policy with the following settings shown.

   This IPv6 explicit web proxy policy allows traffic from all IPv6 IP addresses to connect through the explicit web proxy and through the wan1 interface to any IPv6 addresses that are accessible from the wan1 interface.

If you have enabled both the IPv4 and the IPv6 explicit web proxy, you can combine IPv4 and IPv6 addresses in a single explicit web proxy policy to allow both IPv4 and IPv6 traffic through the proxy.

Example IPv6 Explicit Web Proxy security policy



Restricting the IP address of the explicit IPv6 web proxy

You can use the following command to restrict access to the IPv6 explicit web proxy using only one IPv6 address. The IPv6 address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit web proxy is enabled on an interface with multiple IPv6 addresses.

For example, to require users to connect to the IPv6 address 2001:db8:0:2::30 to connect to the explicit IPv6 HTTP proxy, use the following command:

```
config web-proxy explicit
   set incoming-ipv6 2001:db8:0:2::30
end
```

Restricting the outgoing source IP address of the IPv6 explicit web proxy

You can use the following command to restrict the source address of outgoing web proxy packets to a single IPv6 address. The IP address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit HTTP proxy is enabled on an interface with multiple IPv6 addresses.

For example, to restrict the outgoing packet source address to 2001:db8:0:2::50:

```
config http-proxy explicit
   set outgoing-ip6 2001:db8:0:2::50
end
```

VIP64

VIP64 policies can be used to configure static NAT virtual IPv6 address for IPv4 addresses. VIP64 can be configured from the CLI using the following commands:

```
config firewall vip64
   edit <zname_str>
```

```
    set arp-reply {enable | disable}
    set color <color_int>
    set comment <comment_str>
    set extip <address_ipv6>[-address_ipv6]
    set extport <port_int>
    set id <id_num_str>
    set mappedip [<start_ipv4>-<end_ipv4>]
    set mappedport <port_int>
    set portforward {enable | disable}
    set src-filter <addr_str>
end
```

VIP64 CLI Variables and Defaults

Variable	Description	Default
`<zname_str>`	Enter the name of this virtual IP address.	No default.
`arp-reply {enable | disable}`	Select to respond to ARP requests for this virtual IP address.	enable
`color <color_int>`	Enter the number of the color to use for the group icon in the web-based manager.	0
`comment <comment_str>`	Enter comments relevant to the configured virtual IP.	No default.
`extip <address_ipv6>[-address_ipv6]`	Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network. If `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set `extip` to ::.	::
`extport <port_int>`	Enter the external port number that you want to map to a port number on the destination network. This option only appears if `portforward` is enabled. If `portforward` is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set `extport` to the first port number in the range. Then set `mappedport` to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the `extport` port number range.	0

Variable	Description	Default
`id <id_num_str>`	Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535.	No default.
`mappedip [<start_ipv4>-<end_ipv4>]`	Enter the IP address or IP address range on the destination network to which the external IP address is mapped. If `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. If `mappedip` is an IP address range, the FortiGate unit uses `extip` as a single IP address to create a one-to-many mapping.	0.0.0.0
`mappedport <port_int>`	Enter the port number on the destination network to which the external port number is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network. For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.	0
`portforward {enable | disable}`	Select to enable port forwarding. You must also specify the port forwarding mappings by configuring `extport` and `mappedport`.	disable
`src-filter <addr_str>`	Enter a source address filter. Each address must be in the form of an IPv4 subnet (x:x:x:x:x:x:x:x/n). Separate addresses with spaces.	null

VIP46 policies can be used to configure static NAT virtual IPv4 address for IPv6 addresses. VIP46 can be configured from the CLI using the following commands (see the table below for variable details):

```
config firewall vip46
   edit <name_str>
      set arp-reply {enable | disable}
      set color <color_int>
```

```
    set comment <comment_str>
    set extip <address_ipv4>[-address_ipv4]
    set extport <port_int>
    set id <id_num_str>
    set mappedip [<start_ipv6>-<end_ipv6>]
    set mappedport <port_int>
    set portforward {enable | disable}
    set src-filter <add_str>
end
```

VIP46 CLI Variables and Defaults

Variable	Description	Default
`<name_str>`	Enter the name of this virtual IP address.	No default.
`arp-reply {enable | disable}`	Select to respond to ARP requests for this virtual IP address.	enable
`color <color_int>`	Enter the number of the color to use for the group icon in the web-based manager.	0
`comment <comment_str>`	Enter comments relevant to the configured virtual IP.	No default.
`extip <address_ipv4>[-address_ipv4]`	Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network. If `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set `extip` to 0.0.0.0.	0.0.0.0
`extport <port_int>`	Enter the external port number that you want to map to a port number on the destination network. This option only appears if `portforward` is enabled. If `portforward` is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set `extport` to the first port number in the range. Then set `mappedport` to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the `extport` port number range.	0

Variable	Description	Default
`id <id_num_str>`	Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535.	No default.
`mappedip [<start_ipv6>-<end_ipv6>]`	Enter the IP address or IP address range on the destination network to which the external IP address is mapped. If mappedip is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. If `mappedip` is an IP address range, the FortiGate unit uses `extip` as a single IP address to create a one-to-many mapping.	::
`mappedport <port_int>`	Enter the port number on the destination network to which the external port number is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network. For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.	0
`portforward {enable | disable}`	Select to enable port forwarding. You must also specify the port forwarding mappings by configuring `extport` and `mappedport`.	disable
`src-filter <addr_str>`	Enter a source address filter. Each address must be in the form of an IPv4 subnet (x.x.x.x/n). Separate addresses with spaces.	null

IPv6 Network Address Translation

NAT66, NAT64, and DNS64 are now supported for IPv6. These options provide IPv6 NAT and DNS capabilities withIPv6-IPv4 tunnelling or dual stack configurations. The commands are available only in the CLI.

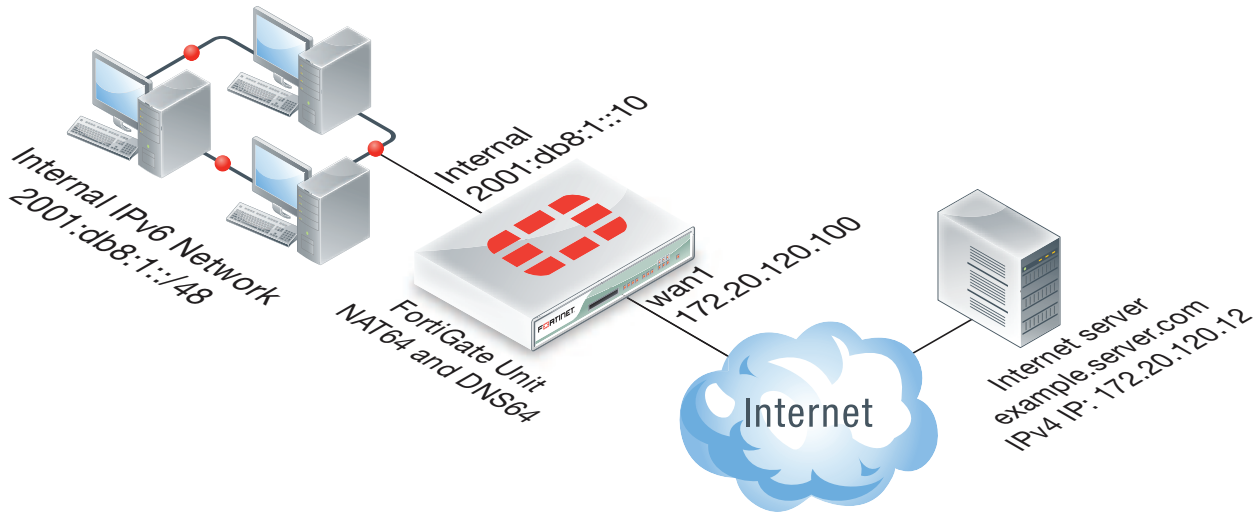
Fortinet supports all features described in RFC 6146. However, for DNS64 there is no support for handling Domain Name System Security Extensions (DNSSEC). DNSSEC is for securing types of information that are provided by the DNS as used on an IP network or networks. You can find more information about DNS64 in RFC 6147.

NAT64 and DNS64 (DNS proxy)

NAT64 is used to translate IPv6 addresses to IPv4 addresses so that a client on an IPv6 network can communicate transparently with a server on an IPv4 network.

NAT64 is usually implemented in combination with the DNS proxy called DNS64. DNS64 synthesizes AAAA records from A records and is used to synthesize IPv6 addresses for hosts that only have IPv4 addresses. 'DNS proxy' and 'DNS64' are interchangeable terms.

Example NAT64 configuration



With a NAT64 and DNS64 configuration in place on a FortiGate unit, clients on an IPv6 network can transparently connect to addresses on an IPv4 network. NAT64 and DNS64 perform the IPv4 to IPv6 transition, allowing clients that have already switched to IPv6 addresses to continue communicating with servers that still use IPv4 addresses.

To enable NAT64 and DNS64, use the following CLI commands:

Enable NAT64

```
config system nat64
   set status enable
end
```

Enable the DNS proxy on the IPv6 interface

```
config system dns-server
   edit internal
   end
```

In your DHCP6 configuration, configure the IPv6 interface IP address as the DNS6 server IP address. The FortiGate will proxy DNS requests to the system DNS server.

```
config system dhcp6 server
   edit 1
      set interface internal
      config ip-range
         edit 1
            set start-ip 2001:db8:1::11
            set end-ip 2001:db8:1::20
         end
      set dns-server1 2001:db8:1::10
   end
```

NAT64 policies

You can configure security policies for NAT64 using the web-based manager. For these options to appear, the feature must be enabled using **Feature Select**. You can then configure the policies under **Policy & Objects > Policy > NAT64**.

NAT64 policies and can also be configured from the CLI using the following command:

```
config firewall policy64
```

In the following section, you will configure a NAT64 policy that allows connections from an internal IPv6 network to an external IPv4 network.

Configuring NAT64 to allow a host on the IPv6 network to connect to the Internet server

In this example, the Internal IPv6 network address is 2001:db8:1::/48 and the external IPv4 network address is 172.20.120.0/24. NAT64 is configured to allow a user on the internal network to connect to the server at IPv4 address 172.20.120.12. In this configuration, sessions exiting the wan1 interface must have their source address changed to an IPv4 address in the range 172.20.120.200 to 172.20.120.210.

Enter the following command to enable NAT64:

```
config system nat64
   set status enable
end
```

Enabling NAT64 with the `config system nat64` command means that all IPv6 traffic received by the current VDOM can be subject to NAT64 if the source and destination address matches an NAT64 security policy.

By default, the setting `always-synthesize-aaaa-record` is enabled. If you disable this setting, the DNS proxy (DNS64) will attempt to find an AAAA records for queries to domain names and therefore resolve the host names to IPv6 addresses. If the DNS proxy cannot find an AAAA record, it synthesizes one by adding the NAT64 prefix to the A record.

By using the `nat64-prefix` option of the `config system nat64` command to change the default nat64 prefix from the well-known prefix of 64:ff9b::/96 and setting `always-synthesize-aaaa-record` to `enable` (default), the DNS proxy does not check for AAAA records but rather synthesizes AAAA records.

As an alternative to the above entry, there is the optional configuration that would allow the resolution of CNAME queries.

```
config system nat64
   set status enable
```

```
    set nat64-prefix 64:ff9b::/96
    set always-synthesize-aaaa-record enable
end
```

Enter the following command to add an IPv6 firewall address for the internal network:

```
config firewall address6
    edit internal-net6
        set ip6 2001:db8:1::/48
    end
```

Enter the following command to add an IPv4 firewall address for the external network:

```
config firewall address
    edit external-net4
        set subnet 172.20.120.0/24
        set associated-interface wan1
    end
```

Enter the following command to add an IP pool containing the IPv4 address that the should become the source address of the packets exiting the wan1 interface:

```
config firewall ippool
    edit exit-pool4
        set startip 172.20.120.200
        set endip 172.20.120.210
    end
```

Enter the following command to add a NAT64 policy that allows connections from the internal IPv6 network to the external IPv4 network:

```
    config firewall policy64
        edit 0
            set srcintf internal
            set srcaddr internal-net6
            set dstintf wan1
            set dstaddr external-net4
            set action accept
            set schedule always
            set service ANY
            set logtraffic enable
            set ippool enable
            set poolname exit-pool4
        end
```

The `srcaddr` can be any IPv6 firewall address and the `dstaddr` can be any IPv4 firewall address.

Other NAT64 policy options include `fixedport`, which can be used to prevent NAT64 from changing the destination port. You can also configure traffic shaping for NAT64 policies.

How a host on the internal IPv6 network communicates with example.server.com that only has IPv4 address on the Internet

1. The host on the internal network does a DNS lookup for example.server.com by sending a DNS query for an AAAA record for example.server.com.
2. The DNS query is intercepted by the FortiGate DNS proxy.
3. The DNS proxy attempts to resolve the query with a DNS server on the Internet and discovers that there are no AAAA records for example.server.com.

4. The previous step is skipped if `always-synthesize-aaaa-record` is enabled.
5. The DNS proxy performs an A-record query for example.server.com and gets back an RRSet containing a single A record with the IPv4 address 172.20.120.12.
6. The DNS proxy then synthesizes an AAAA record. The IPv6 address in the AAAA record begins with the configured NAT64 prefix in the upper 96 bits and the received IPv4 address in the lower 32 bits. By default, the resulting IPv6 address is 64:ff9b::172.20.120.12.
7. The host on the internal network receives the synthetic AAAA record and sends a packet to the destination address 64:ff9b::172.20.120.12.
8. The packet is routed to the FortiGate internal interface where it is accepted by the NAT64 security policy.
9. The FortiGate unit translates the destination address of the packets from IPv6 address 64:ff9b::172.20.120.12 to IPv4 address 172.20.120.12 and translates the source address of the packets to 172.20.120.200 (or another address in the IP pool range) and forwards the packets out the wan1 interface to the Internet.

NAT66

NAT66 is used for translating an IPv6 source or destination address to a different IPv6 source or destination address. NAT66 is not as common or as important as IPv4 NAT, as many IPv6 addresses do not need NAT66 as much as IPv4 NAT. However, NAT66 can be useful for a number of reasons. For example, you may have changed the IP addresses of some devices on your network but want traffic to still appear to be coming from their old addresses. You can use NAT66 to translate the source addresses of packets from the devices to their old source addresses.

In FortiOS, NAT66 options can be added to an IPv6 security policy from the CLI. Configuring NAT66 is very similar to configuring NAT in an IPv4 security policy. For example, use the following command to add an IPv6 security policy that translates the source address of IPv6 packets to the address of the destination interface (similar to IPv4 source NAT:

```
config firewall policy6
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr internal_net
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set nat enable
   end
```

Its also can be useful to translate one IPv6 source address to another address that is not the same as the address of the exiting interface. You can do this using IP pools. For example, enter the following command to add an IPv6 IP pool containing one IPv6 IP address:

```
config firewall ippool6
   edit example_6_pool
      set startip 2001:db8::
      set endip 2001:db8::
   end
```

Enter the following command to add an IPv6 firewall address that contains a single IPv6 IP address.

```
config firewall address6
   edit device_address
      set ip6 2001:db8::132/128
```

```
    end
```

Enter the following command to add an IPv6 security policy that accepts packets from a device with IP address 2001:db8::132 and translates the source address to 2001:db8::.

```
config firewall policy6
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr device_address
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set nat enable
      set ippool enable
      set poolname example_6_pool
   end
```

NAT66 destination address translation

NAT66 can also be used to translate destination addresses. This is done in an IPv6 policy by using IPv6 virtual IPs. For example, enter the following command to add an IPv6 virtual IP that maps the destination address 2001:db8::dd to 2001:db8::ee.

```
config firewall vip6
   edit example-vip6
      set extip 2001:db8::dd
      set mappedip 2001:db8::ee
   end
```

Enter the following command to add an IPv6 security policy that accepts packets with a destination address 2001:db8::dd and translates that destination address to 2001:db8::ee.

```
config firewall policy6
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr all
      set dstaddr example-vip6
      set action accept
      set schedule always
      set service ANY
   end
```

NAT64 and NAT66 session failover

The FortiGate Clustering Protocol (FGCP) supports IPv6, NAT64, and NAT66 session failover. If session pickup is enabled, these sessions are synchronized between cluster members and, after an HA failover, the sessions will resume with only minimal interruption.

NAT46

NAT46 is used to translate IPv4 addresses to IPv6 addresses so that a client on an IPv4 network can communicate transparently with a server on an IPv6 network.

To enable NAT46, use the following CLI command:

```
config firewall vip46
```

NAT46 policies

Security policies for NAT46 can be configured from the web-based manager. For these options to appear in the web-based manager, this feature must be enabled using **Feature Select**. You can then configure the policies under **Policy & Objects > Policy > NAT46**.

NAT46 policies and can also be configured from the CLI using the following command:

```
config firewall policy46
```

ICMPv6

Internet Control Message Protocol version 6 (ICMPv6) is the new implementation of the Internet Control Message Protocol (ICMP) that is part of Internet Protocol version 6 (IPv6). The ICMPv6 protocol is defined in RFC 4443.

ICMPv6 is a multipurpose protocol. It performs such things as:

- error reporting in packet processing
- diagnostic functions
- Neighbor Discovery process
- IPv6 multicast membership reporting

It is also designed as a framework to use extensions for use with future implementations and changes.

Examples of extensions that have already been written for ICMPv6:

- Neighbor Discovery Protocol (NDP) - a node discovery protocol in IPv6 which replaces and enhances functions of ARP.
- Secure Neighbor Discovery Protocol (SEND) - an extension of NDP with extra security.
- Multicast Router Discovery (MRD) - allows discovery of multicast routers.
- ICMPv6 messages use IPv6 packets for transportation and can include IPv6 extension headers. ICMPv6 includes some of the functionality that in IPv4 was distributed among protocols such as ICMPv4, ARP (Address Resolution Protocol), and IGMP (Internet Group Membership Protocol version 3).
- ICMPv6 has simplified the communication process by eliminating obsolete messages.

ICMPv6 messages are subdivided into two classes: error messages and information messages.

Error Messages are divided into four categories:

- Destination Unreachable
- Time Exceeded
- Packet Too Big
- Parameter Problems
- Information messages are divided into three groups:
- Diagnostic messages
- Neighbor Discovery messages
- Messages for the management of multicast groups.

ICMPv6 Types and Codes

ICMPv6 has a number of messages that are identified by the “Type” field. Some of these types have assigned “Code” fields as well. The table below shows the different types of ICMP Types with their associated codes if there are any.

Type codes 0 − 127 are error messages and type codes 128 − 255 are for information messages.

ICMPv6 Types and Codes

Type #	Type Name	Code
0	Reserved	0 - no route to destination 1 - communication with destination administratively prohibited 2 - beyond scope of source address 3 - address unreachable 4 - port unreachable 5 - source address failed ingress/egress policy 6 - reject route to destination 7 - Error in Source Routing Header
1	Destination Unreachable	
2	Packet Too Big	
3	Time Exceeded	0 - hop limit exceeded in transit 1 - fragment reassembly time exceeded
4	Parameter Problem	0 - erroneous header field encountered 1 - unrecognized Next Header type encountered 2 - unrecognized IPv6 option encountered
100	Private Experimentation	
101	Private Experimentation	
102 - 126	Unassigned	
127	Reserved for expansion if ICMPv6 error messages	
128	Echo Request	
129	Echo Replay	
130	Multicast Listener Query	
131	Multicast Listener Report	

Type #	Type Name	Code
132	Multicast Listener Done	
133	Router Solicitation	
134	Router Advertisement	
135	Neighbor Solicitation	
136	Neighbor Advertisement	
137	Redirect Message	
138	Router Renumbering	0 - Router Renumbering Command 1 - Router Renumbering Result 255 - Sequence Number Reset
139	ICMP Node Information Query	0 - The Data field contains an IPv6 address which is the Subject of this Query. 1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP. 2 - The Data field contains an IPv4 address which is the Subject of this Query.
140	ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty. 1 - The Responder refuses to supply the answer. The Reply Data field will be empty. 2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.
141	Inverse Neighbor Discovery Solicitation Message	
142	Inverse Neighbor Discovery Advertisement Message	
143	Version 2 Multicast Listener Report	
144	Home Agent Address Discovery Request Message	

Type #	Type Name	Code
145	Home Agent Address Discovery Reply Message	
146	Mobile Prefix Solicitation	
147	Mobile Prefix Advertisement	
148	Certification Path Solicitation Message	
149	Certification Path Advertisement Message	
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	
151	Multicast Router Advertisement	
152	Multicast Router Solicitation	
153	Multicast Router Termination	
154	FMIPv6 Messages	
155	RPL Control Message	
156	ILNPv6 Locator Update Message	
157	Duplicate Address Request	
158	Duplicate Address Confirmation	
159 – 199	Unassigned	
200	Private experimentation	
201	Private experimentation	
255	Reserved for expansion of ICMPv6 informational messages	

IPv6 in dynamic routing

Unless otherwise stated, routing protocols apply to IPv4 addressing. This is the standard address format used. However, IPv6 is becoming more popular and new versions of the dynamic routing protocols have been introduced.

As with most advanced routing features on your FortiGate unit, IPv6 settings for dynamic routing protocols must be enabled before they will be visible in the GUI. To enable IPv6 configuration in the GUI, enable it in **System > Config > Features**. Alternatively, you can directly configure IPv6 for RIP, BGP, or OSPF protocols using CLI commands.

Dual stack routing

Dual stack routing implements dual IP layers in hosts and routers, supporting both IPv6 and IPv4. A dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, and even maintain some IPv4 support indefinitely if that is necessary. Devices that are on this type of network, and connect to the Internet, can query Internet DNS servers for both IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can easily connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 addresses.

In FortiOS, dual stack architecture it is not comprised merely of basic addressing functions that operate in both versions of IP. The other features of the appliance, such as UTM and routing, can also use both IP stacks.

If an organization with a mixed network uses an Internet service provider that does not support IPv6, they can use an IPv6 tunnel broker to connect to IPv6 addresses that are on the Internet. FortiOS supports IPv6 tunnelling over IPv4 networks to tunnel brokers. The tunnel broker extracts the IPv6 packets from the tunnel and routes them to their destinations.

IPv6 tunnelling

IPv6 Tunnelling is the act of tunnelling IPv6 packets from an IPv6 network through an IPv4 network to another IPv6 network. Unlike NAT, once the packet reaches its final destination, the true originating address of the sender will still be readable. The IPv6 packets are encapsulated within packets with IPv4 headers, which carry their IPv6 payload through the IPv4 network.

The key to IPv6 tunnelling is the ability of the two devices to be dual stack compatible in order to work with both IPv4 and IPv6 at the same time. In the process, the entry node of the tunnel portion of the path will create an encapsulating IPv4 header and transmit the encapsulated packet. The exit node at the end of the tunnel receives the encapsulated packet, removes the IPv4 header, updates the IPv6 header, and processes the packet.

There are two types of tunnels in IPv6:

Automatic tunnels: Automatic tunnels are configured by using IPv4 address information embedded in an IPv6 address – the IPv6 address of the destination host includes information about which IPv4 address the packet should be tunnelled to.

Configured tunnels: Configured tunnels must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified.

Tunnel configuration

There are a few ways in which the tunnelling can be performed depending on which segment of the path between the endpoints of the session the encapsulation takes place.

Host to Host: Dual Stack capable hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire path taken by the IPv6 packets.

Network Device to Host: Dual Stack capable network devices can tunnel IPv6 packets to their final destination IPv6 or IPv4 host. This tunnel spans only the last segment of the path taken by the IPv6 packets.

The node that does the encapsulation needs to maintain soft state information about each tunnel in order to process the IPv6 packets.

Use the following command to tunnel IPv6 traffic over an IPv4 network. The IPv6 interface is configured under `config system interface`. The command to do the reverse is `config system ipv6-tunnel`. These commands are not available in Transparent mode.

```
config system sit-tunnel
   edit <tunnel name>
      set destination <tunnel _address>
      set interface <name>
      set ip6 <address_ipv6>
      set source <address_ipv4>
   end
```

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the IPv6 tunnel.	No default.
`destination <tunnel_ address>`	The destination IPv4 address for this tunnel.	0.0.0.0
`interface <name>`	The interface used to send and receive traffic for this tunnel.	No default.
`ip6 <address_ipv6>`	The IPv6 address for this tunnel.	No default.
`source <address_ipv4>`	The source IPv4 address for this tunnel.	0.0.0.0

Tunnelling IPv6 through IPsec VPN

A variation on tunnelling IPv6 through IPv4 is to use an IPsec VPN tunnel between two FortiGate devices. FortiOS supports IPv6 over IPsec. In this sort of scenario, two networks using IPv6 behind FortiGate units are separated by the Internet, which uses IPv4. An IPsec VPN tunnel is created between the FortiGate units and a tunnel is created over the IPv4-based Internet, but the traffic in the tunnel is IPv6. This has the additional advantage of securing the traffic.

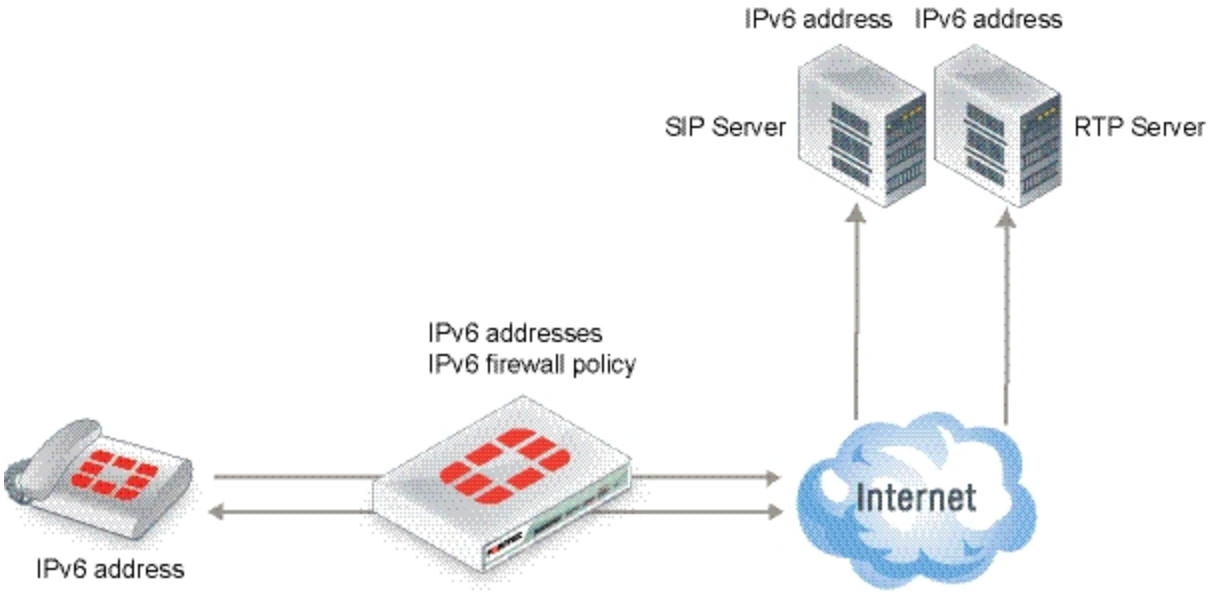
For configuration information, see IPv6 IPsec VPN on page 1813.

SIP over IPv6

FortiOS supports Sessions Initiate Protocol (SIP) over IPv6. The SIP application-level gateway (ALG) can process SIP messages that use IPv6 addresses in the headers, bodies, and in the transport stack. The SIP ALG cannot modify the IPv6 addresses in the SIP headers so FortiGate units cannot perform SIP or RTP NAT over IPv6 and also cannot translate between IPv6 and IPv4 addresses.

In the scenario shown below, a SIP phone connects to the Internet through a FortiGate unit operating. The phone and the SIP and RTP servers all have IPv6 addresses.

The FortiGate unit has IPv6 security policies that accept SIP sessions. The SIP ALG understands IPv6 addresses and can forward IPv6 sessions to their destinations. Using SIP application control features the SIP ALG can also apply rate limiting and other settings to SIP sessions.



To enable SIP support for IPv6 add an IPv6 security policy that accepts SIP packets and includes a VoIP profile.

New Fortinet FortiGate IPv6 MIB fields

The following IPv6 MIB fields have been added to the Fortinet FortiGate MIB. These MIB entries can be used to display IPv6 session and policy statistics.

- IPv6 Session Counters:

```
fgSysSes6Count
fgSysSes6Rate1
fgSysSes6Rate10
fgSysSes6Rate30
fgSysSes6Rate60
```

- IPv6 Policy Statistics:

```
fgFwPol6StatsTable
fgFwPol6StatsEntry
FgFwPol6StatsEntry
fgFwPol6ID
fgFwPol6PktCount
fgFwPol6ByteCount
```

- IPv6 Session Statistics:

```
fgIp6SessStatsTable
fgIp6SessStatsEntry
FgIp6SessStatsEntry
fgIp6SessNumber
```

The fgSysSesCount and fgSysSesRateX MIBs report statistics for IPv4 plus IPv6 sessions combined. This behavior was not changed.

New OIDs

The following OIDs have been added:

```
FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgSystem.fgSystemInfo
.fgSysSes6Count   1.3.6.1.4.1.12356.101.4.1.15
.fgSysSesRate1    1.3.6.1.4.1.12356.101.4.1.16
.fgSysSesRate10   1.3.6.1.4.1.12356.101.4.1.17
.fgSysSesRate30   1.3.6.1.4.1.12356.101.4.1.18
.fgSysSesRate60   1.3.6.1.4.1.12356.101.4.1.19

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies.fgFwPolTables
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6ID   1.3.6.1.4.1.12356.101.5.1.2.2.1.1
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6PktCount   1.3.6.1.4.1.12356.101.5.1.2.2.1.
    2
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6ByteCount   1.3.6.1.4.1.12356.101.5.1.2.2.1
    .3

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgInetProto.fgInetProtoTables
.fgIp6SessStatsTable.fgIp6SessStatsEntry.fgIp6SessNumber 1.3.6.1.4.1.12356.101.11.2.3.1.1
```

EXAMPLE SNMP get/walk output

```
// Session6 stats excerpt from sysinfo:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.4
FORTINET-FORTIGATE-MIB::fgSysSes6Count.0 = Gauge32: 203
FORTINET-FORTIGATE-MIB::fgSysSes6Rate1.0 = Gauge32: 10 Sessions Per Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate10.0 = Gauge32: 2 Sessions Per Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate30.0 = Gauge32: 1 Sessions Per Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate60.0 = Gauge32: 0 Sessions Per Second

// FwPolicy6 table:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.5.1.2.2
FORTINET-FORTIGATE-MIB::fgFwPol6ID.1.3 = INTEGER: 3
FORTINET-FORTIGATE-MIB::fgFwPol6ID.1.4 = INTEGER: 4
FORTINET-FORTIGATE-MIB::fgFwPol6PktCount.1.3 = Counter64: 4329
FORTINET-FORTIGATE-MIB::fgFwPol6PktCount.1.4 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgFwPol6ByteCount.1.3 = Counter64: 317776
FORTINET-FORTIGATE-MIB::fgFwPol6ByteCount.1.4 = Counter64: 0

// IP6SessNumber:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.11.2.3.1
FORTINET-FORTIGATE-MIB::fgIp6SessNumber.1 = Counter32: 89
```

IPv6 Per-IP traffic shaper

You can add any Per-IP traffic shaper to an IPv6 security policy using the following command:

```
config firewall policy6
   edit 0
      set per-ip-shaper "new-perip-shaper"
   end
```

DHCPv6

You can use DHCP with IPv6 using the CLI. To configure DHCP, ensure IPv6 is enabled by going to **System > Config > Features** and enabling **IPv6**.

Use the CLI command

```
config system dhcp6
```

For more information on the configuration options, see the FortiGate CLI Reference.

DHCPv6 relay

You can use the following command to configure a FortiGate interface to relay DHCPv6 queries and responses from one network to a network with a DHCPv6 server and back. The command enables DHCPv6 relay and includes adding the IPv6 address of the DHCP server that the FortiGate unit relays DHCPv6 requests to:

```
config system interface
   edit internal
      config ipv6
         set dhcp6-relay-service enable
         set dhcp6-relay-type regular
         set dhcp6-relay-ip 2001:db8:0:2::30
      end
```

IPv6 forwarding

Policies, IPS, Application Control, flow-based antivirus, web filtering, and DLP

FortiOS fully supports flow-based inspection of IPv6 traffic. This includes full support for IPS, application control, virus scanning, and web filtering.
To add flow-based inspection to IPv6 traffic go to **Policy & Objects > Policy > IPv6** and select **Create New** to add an IPv6 Security Policy. Configure the policy to accept the traffic to be scanned. Under **Security Profiles**, select the profiles to apply to the traffic.

Obtaining IPv6 addresses from an IPv6 DHCP server

From the CLI, you can configure any FortiGate interface to get an IPv6 address from an IPv6 DHCP server. For example, to configure the wan2 interface to get an IPv6 address from an IPv6 DHCP server enter the following command:

```
config system interface
   edit wan2
      config ipv6
         set ip6-mode dhcp
      end
```

IPv6 Configuration

This section contains configuration information for IPv6 on FortiOS. Attempts are made to include scenarios in each section to better assist with the configuration and to orient the information toward a particular task.

You will find information on the following:

IPv6 address groups
IPv6 address ranges
IPv6 firewall addresses
ICMPv6
IPv6 IPsec VPN
TCP MSS values
BGP and IPv6
RIPng — RIP and IPv6
IPv6 RSSO support
IPv6 IPS
Blocking IPv6 packets by extension headers
IPv6 Denial of Service policies
Configure hosts in an SNMP v1/2c community to send queries or receive traps
IPv6 PIM sparse mode multicast routing

By default IPv6 configurations do not appear in the web-based manager. You need to enable the feature first.

To enable IPv6:

1. Go to **System > Config > Features**.
2. Select **IPv6** and click **Apply**.

IPv6 address groups

To create IPv6 address groups from existing IPv6 addresses - web-based manager

Your company has 3 internal servers with IPv6 addresses that it would like to group together for the purposes of a number of policies.

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New > Address Group.**
2. Select **IPv6 Group**, and fill out the fields with the following information:

Group Name	Web_Server_Cluster

Members	Web_Server-1
	Web_Server-2
	Web_Server-3

3. Select **OK.**

To create IPv6 address groups from existing IPv6 addresses - CLI

```
config firewall addrgrp6
   edit Web_Server_Cluster
      set member Web_Server-1 Web_Server-2 Web_Server-3
   end
```

To verify that the addresses were added correctly

1. Go to **Policy & Objects > Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. From the CLI, enter the following commands:

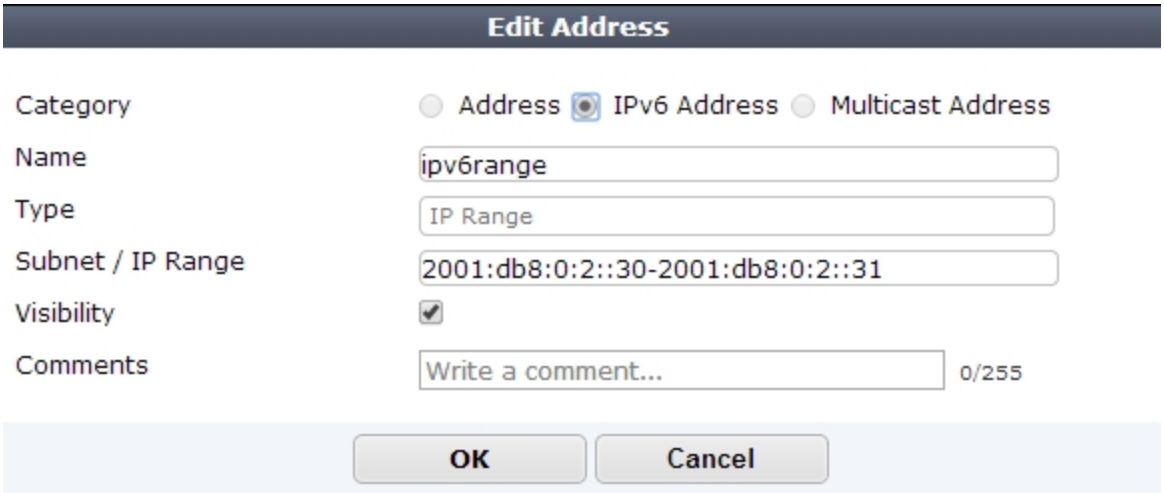
```
config firewall addgrp6
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

IPv6 address ranges

You can configure IPv6 address ranges in both the GUI and the CLI.

To configure IPv6 address ranges - web-based manager:

1. Go to **Policy & Objects > Objects > Addresses.**
2. Set the **Type** to **IP Range** and enter the IPv6 addresses as shown:



To configure IPv6 address ranges - CLI:

```
config firewall address6
   edit ipv6range
```

```
    set type iprange
    set start-ip 2001:db8:0:2::30
    set end-ip 2001:db8:0:2::31
end
```

IPv6 firewall addresses

Scenario: Mail Server

You need to create an IPv6 address for the Mail Server on Port1 of your internal network. This server is on the network off of port1.

- The IP address is 2001:db8:0:2::20/128
- There should be a tag for this address being for a server.

Configuring the Example using the GUI

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New > Address.**
2. Select **IPv6 Address** and fill out the fields with the following information

Name	Mail_Server
Type	Subnet
IPv6 Address	2001:db8:0:2::20/128

3. Select **OK.**

Configuring the Example using the CLI

Enter the following CLI command:

```
config firewall address6
   edit Mail_Server
      set type ipprefix
      set subnet 2001:db8:0:2::20/128
   end
```

Scenario: First Floor Network

You need to create an IPv6 address for the subnet of the internal network off of Port1. These computers connect to port1. The network uses the IPv6 addresses: fdde:5a7d:f40b:2e9d:xxxx:xxxx:xxxx:xxxx

There should be a reference to this being the network for the 1st floor of the building.

1. Go to **Policy & Objects > Objects > Addresses**
2. Select **Create New > Address.**Select **IPv6 Address** and fill out the fields with the following information:

Name	Internal_Subnet_1
Type	Subnet / IP Range

IPv6 Address	2001:db8:0:2::/64
Comments	Network for 1st Floor

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall address6
   edit Internal_Subnet_1
      set comment "Network for 1st Floor"
      set type ipprefix
      set subnet 2001:db8:0:2::/64
   end
```

Scenario: Accounting Team

You need to create an IPv6 address for the Accounting Team that's on the 1st Floor. These users are off of various ports of the FortiGate, but they have all been assigned addresses between 2001:db8:0:2::2000 and 2001:db8:0:2::a000

Configuring the Example using the GUI

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New > Address.**
2. Select **IPv6 Address** and fill out the fields with the following information

Name	Accounting_Team
Type	IP Range
Subnet / IP Range	2001:db8:0:2::2000-2001:db8:0:2::a000

3. Select **OK.**

Configuring the Example using the CLI

Enter the following CLI command:

```
config firewall address6
   edit Accounting_Team
      set type iprange
      set visibility enable
      set start-ip 2001:db8:0:2::2000
      set end-ip 2001:db8:0:2::a000
      end
```

To verify that the addresses were added correctly:

1. Go to **Policy & Objects > Objects > Addresses.** Check that the addresses have been added to the address list and that they are correct.
2. Enter the following CLI command:

```
config firewall address6
   edit <the name of the address that you wish to verify>
      Show full-configuration
```

ICMPv6

The IT Manager is doing some diagnostics and would like to temporarily block the successful replies of ICMP Node information Responses between 2 IPv6 networks.

The ICMP type for ICMP Node informations responses is 140. The codes for a successful response is 0.

To configure ICMPv6 - web-based manager:

1. Go to **Policy & Objects > Objects > Services** and select **Create New > Service**.
2. Fill out the fields with the following information

Name	diagnostic-test1
Service Type	Firewall
Show in Service List	Enabled
Category	Uncategorized
Protocol Type	ICMP6
Type	140

3. Select **OK.**
4. Enter the following CLI command:

```
config firewall service custom
   edit diagnostic-test1
      set protocol ICMP6
      set icmptype 140
      set icmpcode 0
      set visibility enable
   end
```

To verify that the category was added correctly:

1. Go to **Policy & Objects > Objects > Services.**Check that the services have been added to the services list and that they are correct.
2. Enter the following CLI command:

```
config firewall service custom
   edit <the name of the service that you wish to verify>
      show full-configuration
```

IPv6 IPsec VPN

This chapter describes how to configure your FortiGate unit's IPv6 IPsec VPN functionality.

By default IPv6 configurations do not appear in the web-based manager. You need to enable the feature first.

To enable IPv6:

1. Go to **System > Config > Features**.
2. Select **IPv6** and click **Apply**.

The topics in this section include:

- Overview of IPv6 IPsec support
- Configuring IPv6 IPsec VPNs
- Site-to-site IPv6 over IPv6 VPN example
- Site-to-site IPv4 over IPv6 VPN example
- Site-to-site IPv6 over IPv4 VPN example

Overview of IPv6 IPsec support

FortiOS supports route-based IPv6 IPsec, but not policy-based. This section describes how IPv6 IPsec support differs from IPv4 IPsec support.

Where both the gateways and the protected networks use IPv6 addresses, sometimes called IPv6 over IPv6, you can create either an auto-keyed or manually-keyed VPN. You can also combine IPv6 and IPv4 addressing in an auto-keyed VPN in the following ways:

IPv4 over IPv6	The VPN gateways have IPv6 addresses. The protected networks have IPv4 addresses. The phase 2 configurations at either end use IPv4 selectors.
IPv6 over IPv4	The VPN gateways have IPv4 addresses. The protected networks use IPv6 addresses. The phase 2 configurations at either end use IPv6 selectors.

Compared with IPv4 IPsec VPN functionality, there are some limitations:

- Except for IPv6 over IPv4, remote gateways with Dynamic DNS are not supported.
- Selectors cannot be firewall address names. Only IP address, address range and subnet are supported.
- Redundant IPv6 tunnels are not supported.

Certificates

On a VPN with IPv6 phase 1 configuration, you can authenticate using VPN certificates in which the common name (cn) is an IPv6 address. The `cn-type` keyword of the `user peer` command has an option, `ipv6`, to support this.

Configuring IPv6 IPsec VPNs

Configuration of an IPv6 IPsec VPN follows the same sequence as for an IPv4 route-based VPN: phase 1 settings, phase 2 settings, security policies, and routing.

Phase 1 configuration

In the web-based manager, you define the Phase 1 as IPv6 in the Advanced settings. Enable the IPv6 Version check box. You can then enter an IPv6 address for the remote gateway.

In the CLI, you define an IPsec phase 1 configuration as IPv6 by setting `ip-version` to `6`. Its default value is `4`. Then, the `local-gw` and `remote-gw` keywords are hidden and the corresponding `local-gw6` and `remote-gw6` keywords are available. The values for `local-gw6` and `remote-gw6` must be IPv6 addresses. For example:

```
config vpn ipsec phase1-interface
   edit tunnel6
      set ip-version 6
      set remote-gw6 0:123:4567::1234
      set interface port3
      set proposal 3des-md5
   end
```

Phase 2 configuration

To create an IPv6 IPsec phase 2 configuration in the web-based manager, you need to define IPv6 selectors in the Advanced settings. Change the default “0.0.0.0/0” address for Source address and Destination address to the IPv6 value “::/0”. If needed, enter specific IPv6 addresses, address ranges or subnet addresses in these fields.

In the CLI, set `src-addr-type` and `dst-addr-type` to `ip6`, `range6` or `subnet6` to specify IPv6 selectors. By default, zero selectors are entered, “::/0” for the `subnet6` address type, for example. The simplest IPv6 phase 2 configuration looks like this:

```
config vpn ipsec phase2-interface
   edit tunnel6_p2
      set phase1name tunnel6
      set proposal 3des-md5
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
```

Security policies

To complete the VPN configuration, you need a security policy in each direction to permit traffic between the protected network’s port and the IPsec interface. You need IPv6 policies unless the VPN is IPv4 over IPv6.

Routing

Appropriate routing is needed for both the IPsec packets and the encapsulated traffic within them. You need a route, which could be the default route, to the remote VPN gateway via the appropriate interface. You also need a route to the remote protected network via the IPsec interface.

To create a static route - web-based manager:

1. Go to **Router > Static > Static Routes**.

On some desktop FortiGate models, go to **System > Network > Routing**.

2. Select the drop-down arrow on the **Create New** button and select **IPv6 Route**.
3. Enter the information and select **OK**.

To create a static route - CLI:

1. In the CLI, use the `router static6` command. For example, where the remote network is `fec0:0000:0000:0004::/64` and the IPsec interface is `toB`:

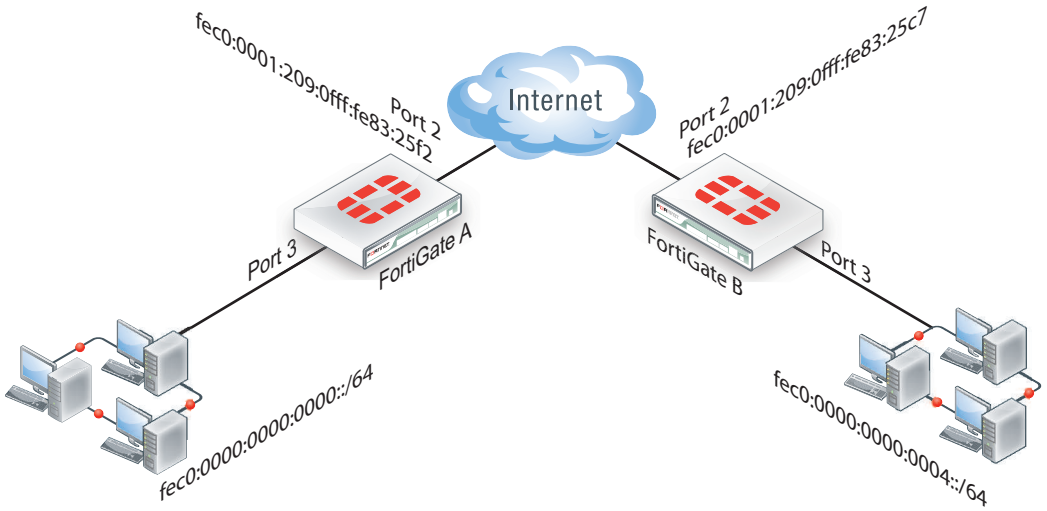
```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toB
      set dst fec0:0000:0000:0004::/64
   next
end
```

If the VPN is IPV4 over IPv6, the route to the remote protected network is an IPv4 route. If the VPN is IPv6 over IPv4, the route to the remote VPN gateway is an IPv4 route.

Site-to-site IPv6 over IPv6 VPN example

In this example, computers on IPv6-addressed private networks communicate securely over public IPv6 infrastructure.

Example IPv6-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the public network and port 3 connects to the local network.

```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0001:209:0fff:fe83:25f2/64
```

```
      end
    next
    edit port3
      config ipv6
        set ip6-address fec0::0000:209:0fff:fe83:25f3/64
      end
    next
end
```

Configure FortiGate A IPsec settings

The phase 1 configuration creates a virtual IPsec interface on port 2 and sets the remote gateway to the public IP address FortiGate B. This configuration is the same as for an IPv4 route-based VPN, except that `ip-version` is set to `6` and the `remote-gw6` keyword is used to specify an IPv6 remote gateway address.

```
config vpn ipsec phase1-interface
  edit toB
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
```

By default, phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
  edit toB2
    set phase1name toB
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
```

Configure FortiGate A security policies

Security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. The address `all6` must be defined using the `firewall address6` command as `::/0`.

```
config firewall policy6
  edit 1
    set srcintf port3
    set dstintf toB
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toB
    set dstintf port3
    set srcaddr all6
```

```
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB. A default route sends all IPv6 traffic out on port2.

```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toB
      set dst fec0:0000:0000:0004::/64
   end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. Security policies enable traffic to pass between the private network and the IPsec interface. Routing ensures traffic for the private network behind FortiGate A goes through the VPN and that all IPv6 packets are routed to the public network.

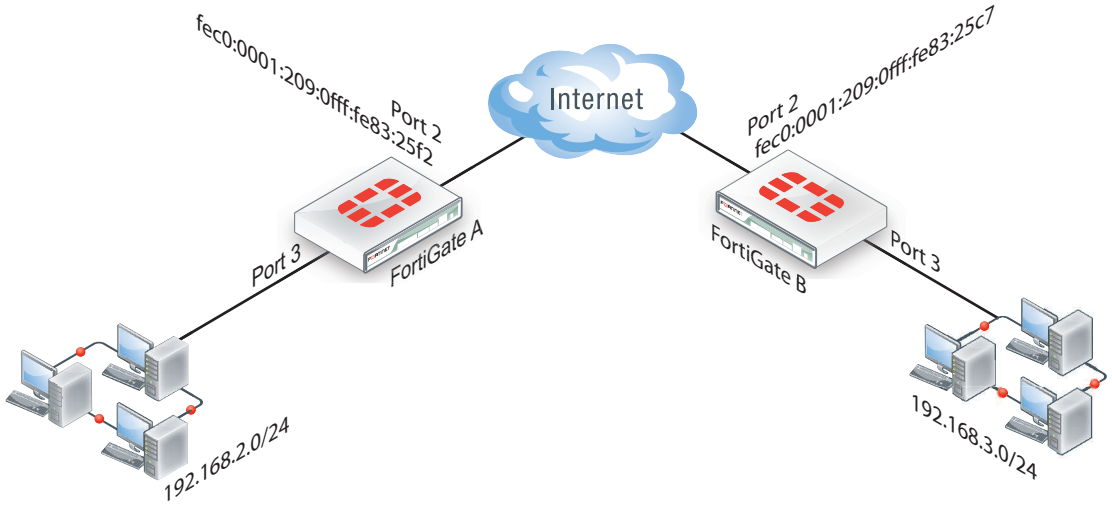
```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0003:209:0fff:fe83:25c7/64
      end
   next
   edit port3
      config ipv6
         set ip6-address fec0::0004:209:0fff:fe83:2569/64
      end
   end
config vpn ipsec phase1-interface
   edit toA
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
```

```
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toA
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toA
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toA
      set dst fec0:0000:0000:0000::/64
end
```

Site-to-site IPv4 over IPv6 VPN example

In this example, two private networks with IPv4 addressing communicate securely over IPv6 infrastructure.

Example IPv4-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv6 public network and port 3 connects to the IPv4 LAN.

```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0001:209:0fff:fe83:25f2/64
      end
   next
   edit port3
      set 192.168.2.1/24
   end
```

Configure FortiGate A IPsec settings

The phase 1 configuration is the same as in the IPv6 over IPv6 example.

```
config vpn ipsec phase1-interface
   edit toB
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
```

The phase 2 configuration is the same as you would use for an IPv4 VPN. By default, phase 2 selectors are set to accept all subnet addresses for source and destination.

```
config vpn ipsec phase2-interface
   edit toB2
      set phase1name toB
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
   end
```

Configure FortiGate A security policies

Security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. These are IPv4 security policies.

```
config firewall policy
   edit 1
      set srcintf port3
      set dstintf toB
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toB
      set dstintf port3
      set srcaddr all
      set dstaddr all
      set action accept
      set service ANY
      set schedule always
```

```
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB using an IPv4 static route. A default route sends all IPv6 traffic, including the IPv6 IPsec packets, out on port2.

```
config router static6
   edit 1
      set device port2
      set dst 0::/0
   next
   edit 2
      set device toB
      set dst 192.168.3.0/24
   end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. The IPsec phase 2 configuration has IPv4 selectors.

IPv4 security policies enable traffic to pass between the private network and the IPsec interface. An IPv4 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv6 static route ensures that all IPv6 packets are routed to the public network.

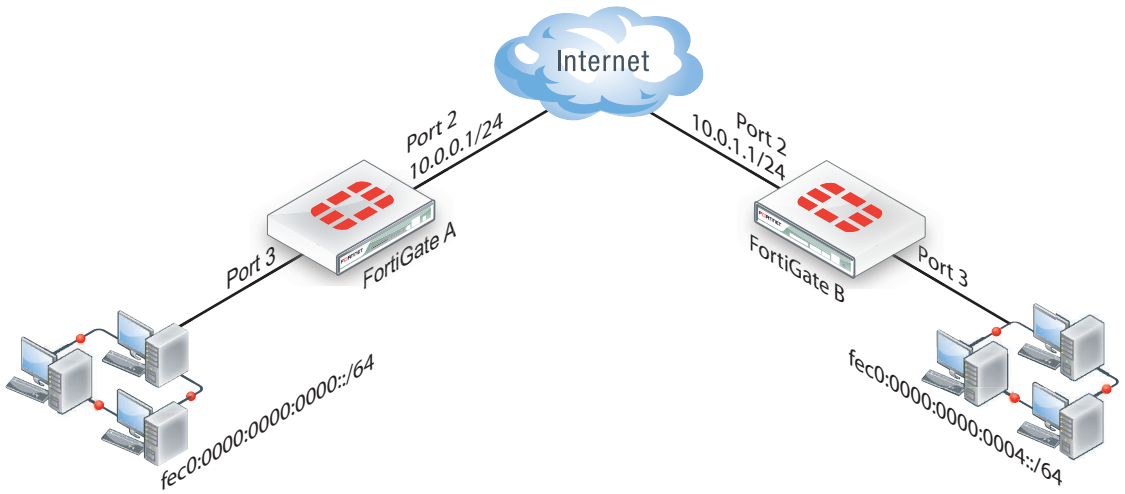
```
config system interface
   edit port2
      config ipv6
         set ip6-address fec0::0003:fe83:25c7/64
      end
   next
   edit port3
      set 192.168.3.1/24
   end
config vpn ipsec phase1-interface
   edit toA
      set ip-version 6
      set interface port2
      set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
   end
config firewall policy
   edit 1
      set srcintf port3
      set dstintf toA
```

```
        set srcaddr all
        set dstaddr all
        set action accept
        set service ANY
        set schedule always
    next
    edit 2
        set srcintf toA
        set dstintf port3
        set srcaddr all
        set dstaddr all
        set action accept
        set service ANY
        set schedule always
    end
config router static6
    edit 1
        set device port2
        set dst 0::/0
    next
    edit 2
        set device toA
        set dst 192.168.2.0/24
    end
```

Site-to-site IPv6 over IPv4 VPN example

In this example, IPv6-addressed private networks communicate securely over IPv4 public infrastructure.

Example IPv6-over-IPv4 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv4 public network and port 3 connects to the IPv6 LAN.

```
config system interface
    edit port2
        set 10.0.0.1/24
        next
```

```
edit port3
config ipv6
   set ip6-address fec0::0001:209:0fff:fe83:25f3/64
end
```

Configure FortiGate A IPsec settings

The phase 1 configuration uses IPv4 addressing.

```
config vpn ipsec phase1-interface
   edit toB
      set interface port2
      set remote-gw 10.0.1.1
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
```

The phase 2 configuration uses IPv6 selectors. By default, phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet6`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
   edit toB2
      set phase1name toB
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
```

Configure FortiGate A security policies

IPv6 security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. Define the address `all6` using the `firewall address6` command as `::/0`.

```
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toB
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toB
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPsec interface toB using an IPv6 static route. A default route sends all IPv4 traffic, including the IPv4 IPsec packets, out on port2.

```
config router static6
   edit 1
      set device toB
      set dst fec0:0000:0000:0004::/64
   end
config router static
   edit 1
      set device port2
      set dst 0.0.0.0/0
      set gateway 10.0.0.254
   end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPsec interface toA is configured on port2 and its remote gateway is the IPv4 public IP address of FortiGate A. The IPsec phase 2 configuration has IPv6 selectors.

IPv6 security policies enable traffic to pass between the private network and the IPsec interface. An IPv6 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv4 static route ensures that all IPv4 packets are routed to the public network.

```
config system interface
   edit port2
      set 10.0.1.1/24
   next
   edit port3
      config ipv6
         set ip6-address fec0::0004:209:0fff:fe83:2569/64
      end
config vpn ipsec phase1-interface
   edit toA
      set interface port2
      set remote-gw 10.0.0.1
      set dpd enable
      set psksecret maryhadalittlelamb
      set proposal 3des-md5 3des-sha1
   end
config vpn ipsec phase2-interface
   edit toA2
      set phase1name toA
      set proposal 3des-md5 3des-sha1
      set pfs enable
      set replay enable
      set src-addr-type subnet6
      set dst-addr-type subnet6
   end
config firewall policy6
   edit 1
      set srcintf port3
      set dstintf toA
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   next
   edit 2
      set srcintf toA
      set dstintf port3
      set srcaddr all6
      set dstaddr all6
      set action accept
      set service ANY
      set schedule always
   end
config router static6
   edit 1
      set device toA
```

```
      set dst fec0:0000:0000:0000::/64
   end
config router static
   edit 1
      set device port2
      set gateway 10.0.1.254
   end
```

TCP MSS values

TCP MSS values, which control the maximum amount of data that can be sent in a single packet, can be set for IPv6 policies (for both the sender and the receiver). You can configure TCP MSS values in IPv6 using the following CLI commands:

```
config firewall policy6
   edit <index_int>
      set tcp-mss-sender <value>
      set tcp-mss-receiver <value>
   end
```

BGP and IPv6

FortiGate units support IPv6 over BGP using the same `config router bgp` command as IPv4, but different subcommands.

The main CLI keywords have IPv6 equivalents that are identified by the “6” on the end of the keyword, such as with `config network6` or `set allowas-in6`.

IPv6 BGP commands include:

```
config router bgp
   set activate6 {enable | disable}
   set allowas-in6 <max_num_AS_integer>
   set allowas-in-enable6 {enable | disable}
   set as-override6 {enable | disable}
   set attribute-unchanged6 [as-path] [med] [next-hop]
   set capability-default-originate6 {enable | disable}
   set capability-graceful-restart6 {enable | disable}
   set default-originate-route-map6 <routemap_str>
   set distribute-list-in6 <access-list-name_str>
   set distribute-list-out6 <access-list-name_str>
   set filter-list-in6 <aspath-list-name_str>
   set filter-list-out6 <aspath-list-name_str>
   set maximum-prefix6 <prefix_integer>
   set maximum-prefix-threshold6 <percentage_integer>
   set maximum-prefix-warning-only6 {enable | disable}
   set next-hop-self6 {enable | disable}
   set prefix-list-in6 <prefix-list-name_str>
   set prefix-list-out6 <prefix-list-name_str>
   set remove-private-as6 {enable | disable}
   set route-map-in6 <routemap-name_str>
   set route-map-out6 <routemap-name_str>
   set route-reflector-client6 {enable | disable}
   set route-server-client6 {enable | disable}
   set send-community6 {both | disable | extended | standard}
   set soft-reconfiguration6 {enable | disable}
   set unsuppress-map6 <route-map-name_str>
```

```
    config network6
    config redistribute6
end
```

RIPng — RIP and IPv6

RIP next generation, or RIPng, is the version of RIP that supports IPv6.

This is an example of a typical small network configuration using RIPng routing.

Your internal R&D network is working on a project for a large international telecom company that uses IPv6. For this reason, you have to run IPv6 on your internal network and you have decided to use only IPv6 addresses.

Your network has two FortiGate units running the RIPng dynamic routing protocol. Both FortiGate units are connected to the ISP router and the internal network. This configuration provides some redundancy for the R&D internal network enabling it to reach the internet at all times.

This section includes the following topics:

- Network layout and assumptions
- Configuring the FortiGate units system information
- Configuring RIPng on FortiGate units
- Configuring other network devices
- Testing the configuration
- Debugging IPv6 on RIPng

Network layout and assumptions

Basic network layout

Your internal R&D network is working on a project for a large international telecom company that uses IPv6. For this reason, you have to run IPv6 on your internal network and you have decided to use only IPv6 addresses.

Your network has two FortiGate units running the RIPng dynamic routing protocol. Both FortiGate units are connected to the ISP router and the internal network. This configuration provides some redundancy for the R&D internal network enabling it to reach the internet at all times.

All internal computers use RIP routing, so no static routing is required. And all internal computers use IPv6 addresses.

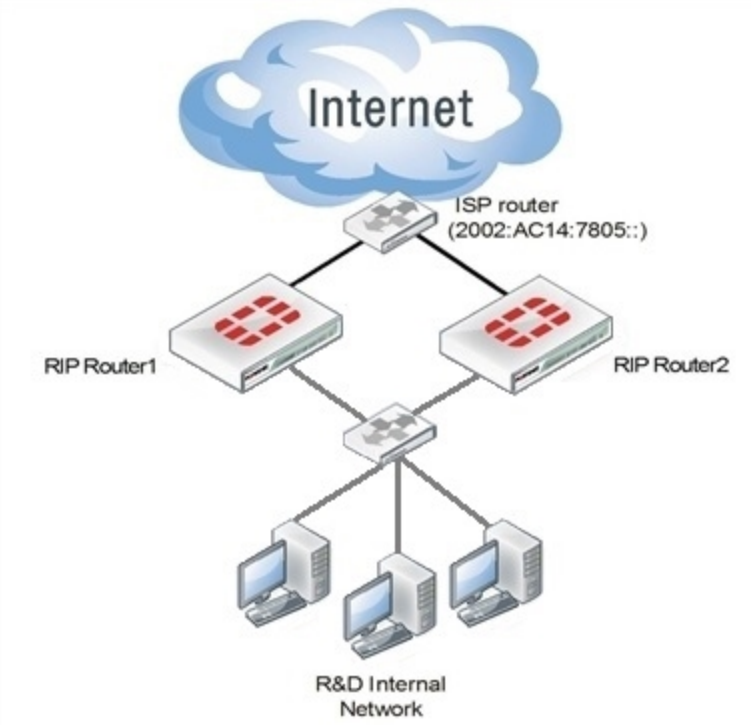
Where possible in this example, the default values will be used or the most general settings. This is intended to provide an easier configuration that will require less troubleshooting.

In this example the routers, networks, interfaces used, and IP addresses are as follows:

Rip example network topology

Network	Router	Interface & Alias	IPv6 address
R&D	Router1	port1 (internal)	2002:A0B:6565:0:0:0:0:0
		port2 (ISP)	2002:AC14:7865:0:0:0:0:0
	Router2	port1 (internal)	2002:A0B:6566:0:0:0:0:0
		port2 (ISP)	2002:AC14:7866:0:0:0:0:0

Network topology for the IPv6 RIPng example



Assumptions

The following assumptions have been made concerning this example:

- All FortiGate units have 5.0+ firmware, and are running factory default settings.
- All CLI and web-based manager navigation assumes the unit is running in NAT/Route operating mode, with VDOMs disabled.
- All FortiGate units have interfaces labelled port1 and port2 as required.
- All firewalls have been configured for each FortiGate unit to allow the required traffic to flow across interfaces.
- All network devices are support IPv6 and are running RIPng.

Configuring the FortiGate units system information

Each FortiGate unit needs IPv6 enabled, a new hostname, and interfaces configured.

To configure system information on Router1 - web-based manager:

1. Go to **System > Dashboard > Status**.
2. For **Host name**, select **Change**.
3. Enter “Router1”.
4. Go to **System > Config > Features**.
5. Enable **IPv6** and click **Apply**.
6. Go to **System > Network > Interfaces**.
7. Edit port1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Netmask	2002:A0B:6565::/0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

9. Edit port2 (ISP) interface.
10. Set the following information, and select **OK**.

Alias	ISP
IP/Netmask	2002:AC14:7865::/0
Administrative Access	HTTPS SSH PING
Description	ISP and internet
Administrative Status	Up

To configure system information on Router1 - CLI:

```
config system global
   set hostname Router1
   set gui-ipv6 enable
end
config system interface
   edit port1
      set alias internal
      set allowaccess https ping ssh
      set description "Internal RnD network"
      config ipv6
         set ip6-address 2002:a0b:6565::/0
      end
   next
   edit port2
      set alias ISP
      set allowaccess https ping ssh
      set description "ISP and internet"
```

```
      config ipv6
         set ip6-address 2002:AC14:7865::
      end
   end
```

To configure system information on Router2 - web-based manager:

1. Go to **System > Dashboard > Status**.
2. For **Host name**, select **Change**.
3. Enter “Router2”.
4. Go to **System > Config > Features**.
5. Enable **IPv6** and click **Apply**.
6. Go to **System > Network > Interfaces**.
7. Edit port1 (internal) interface.
8. Set the following information, and select **OK**.

Alias	internal
IP/Netmask	2002:A0B:6566::/0
Administrative Access	HTTPS SSH PING
Description	Internal RnD network
Administrative Status	Up

9. Edit port2 (ISP) interface.
10. Set the following information, and select **OK**.

Alias	ISP
IP/Netmask	2002:AC14:7866::/0
Administrative Access	HTTPS SSH PING
Description	ISP and internet
Administrative Status	Up

To configure system information on Router2 - CLI:

```
config system global
   set hostname Router2
   set gui-ipv6 enable
end
config system interface
   edit port1
      set alias internal
      set allowaccess https ping ssh
      set description "Internal RnD network"
      config ipv6
         set ip6-address 2002:a0b:6566::/0
      end
```

```
next
edit port2
   set alias ISP
   set allowaccess https ping ssh
   set description "ISP and internet"
   config ipv6
      set ip6-address 2002:AC14:7866::
   end
end
```

Configuring RIPng on FortiGate units

Now that the interfaces are configured, you can configure RIPng on the FortiGate units.

There are only two networks and two interfaces to include — the internal network, and the ISP network. There is no redistribution, and no authentication. In RIPng there is no specific command to include a subnet in the RIP broadcasts. There is also no information required for the interfaces beyond including their name.

As this is a CLI only configuration, configure the ISP router and the other FortiGate unit as neighbors. This was not part of the previous example as this feature is not offered in the web-based manager. Declaring neighbors in the configuration like this will reduce the discovery traffic when the routers start up.

Since RIPng is not supported in the web-based manager, this section will only be entered in the CLI.

To configure RIPng on Router1 - CLI:

```
config router ripng
   config interface
      edit port1
      next
      edit port2
      end
   config neighbor
      edit 1
         set interface port1
         set ipv6 2002:a0b:6566::/0
      next
      edit 2
         set interface port2
         set ipv6 2002:AC14:7805::/0
      end
```

To configure RIPng on Router2 - CLI:

```
config router ripng
   config interface
      edit port1
      next
      edit port2
      end
   config neighbor
      edit 1
         set interface port1
         set ipv6 2002:a0b:6565::/0
      next
      edit 2
         set interface port2
```

```
    set ipv6 2002:AC14:7805::/0
end
```

Configuring other network devices

The other devices on the internal network all support IPv6, and are running RIPng where applicable. They only need to know the internal interface network addresses of the FortiGate units.

The ISP routers need to know the FortiGate unit information such as IPv6 addresses.

Testing the configuration

In addition to normal testing of your network configuration, you must also test the IPv6 part of this example.

For troubleshooting problems with your network, see the FortiOS Handbook Troubleshooting chapter.

Testing the IPv6 RIPng information

There are some commands to use when checking that your RIPng information is correct on your network. These are useful to check on your RIPng FortiGate units on your network. Comparing the output between devices will help you understand your network better, and also track down any problems.

`diagnose ipv6 address list`

View the local scope IPv6 addresses used as next-hops by RIPng on the FortiGate unit.

`diagnose ipv6 route list`

View ipv6 addresses that are installed in the routing table.

`get router info6 routing-table`

View the routing table. This information is almost the same as the previous command (diagnose ipv6 route list) however it is presented in an easier to read format.

`get router info6 rip interface external`

View brief output on the RIP information for the interface listed. The information includes if the interface is up or down, what routing protocol is being used, and whether passive interface or split horizon are enabled.

`get router info6 neighbor-cache list`

View the IPv6/MAC address mapping. This also displays the interface index and name associated with the address.

Debugging IPv6 on RIPng

The debug commands are very useful to see what is happening on the network at the packet level. There are a few changes to debugging the packet flow when debugging IPv6.

The following CLI commands specify both IPv6 and RIP, so only RIPng packets will be reported. The output from these commands will show you the RIPng traffic on your FortiGate unit including RECV, SEND, and UPDATE actions.

The addresses are in IPv6 format.

```
diagnose debug enable
diagnose ipv6 router rip level info
diagnose ipv6 router rip all enable
```

These three commands will:

Turn on debugging in general

Set the debug level to information, a verbose reporting level

Turn on all RIP router settings

Part of the information displayed from the debugging is the metric (hop count). If the metric is 16, then that destination is unreachable since the maximum hop count is 15.

In general, you should see an update announcement, followed by the routing table being sent out, and a received reply in response.

IPv6 RSSO support

RADIUS Single Sign-On (RSSO) is supported in IPv6, but can only be configured in the CLI:

```
config firewall policy6
   edit <id>
      set rsso enable
      set fall-through-unathenticated enable
   end
```

IPv6 IPS

IPv6 IPS signature scan can be enabled by interface policy. The user can create an normal IPS sensor and assign it to the IPv6 interface policy.

```
config firewall interface-policy6
   edit 1
      set interface "port1"
      set srcaddr6 "all"
      set dstaddr6 "all"
      set service6 "ANY"
      set ips-sensor-status enable
      set ips-sensor "all_default"
   next
end
```

Blocking IPv6 packets by extension headers

FortiOS can now block IPv6 packets based on the extension headers, using the CLI syntax:

```
config firewall ipv6-eh-filter.
```

The following commands are now available:

- `set hop-opt {disable | enable}`: Block packets with Hop-by-Hop Options header.
- `set dest-opt {disable | enable}`: Block packets with Destination Options header.
- `set hdopt-type <integer>`: Block specific Hop-by-Hop and/or Destination Option types (maximum 7 types, each between 0 and 255).
- `set routing {disable | enable}`: Block packets with Routing header.
- `set routing-type <integar>`: Block specific Routing header types (maximum 7 types, each between 0 and 255).
- `set fragment {disable | enable}`: Block packets with Fragment header.
- `set auth {disable | enable}`: Block packets with Authentication header.
- `set no-next {disable | enable}`: Block packets with No Next header.

IPv6 Denial of Service policies

Denial of Service (DoS) policies can now be configured by going to **Policy & Objects > Policy > IPv6 DoS**. For more information, refer to the “Interface Policies” section of the FortiOS Handbook Firewall chapter.

Configure hosts in an SNMP v1/2c community to send queries or receive traps

When you add a host to an SNMP v1/2c community you can now decide whether the FortiGate unit will accept queries from the host or whether the FortiGate unit will send traps to the host. You can also configure the host for both traps and queries. You can add up to 16 IPv4 hosts and up to 16 IPv6 hosts.

Use the following command to add two hosts to an SNMP community:

```
config system snmp community
   config hosts
      edit 1
         set interface port1
         set ip 172.20.120.1
         set host-type query
      end
   config hosts6
      edit 1
         set interface port6
         set ip 2001:db8:0:2::30
         set host-type trap
      end
```

IPv6 PIM sparse mode multicast routing

FortiOS supports PIM sparse mode multicast routing for IPv6 multicast (multicast6) traffic and is compliant with RFC 4601. You can use the following command to configure IPv6 PIM sparse multicast routing.

```
config router multicast6
   set multicast-routing {enable | disable}
      config interface
         edit <interface-name>
            set hello-interval <1-65535 seconds>
            set hello-holdtime <1-65535 seconds>
      end
      config pim-sm-global
      config rp-address
         edit <index>
            set ipv6-address <ipv6-address>
      end
```

The following diagnose commands for IPv6 PIM sparse mode are also available:

```
diagnose ipv6 multicast status
diagnose ipv6 multicast vif
diagnose ipv6 multicast mroute
```

Chapter 16 - Life of a Packet

Life of a Packet

Directed by security policies, a FortiGate unit screens network traffic from the IP layer up through the application layer of the TCP/IP stack. This chapter provides a general, high-level description of what happens to a packet as it travels through a FortiGate unit running FortiOS 5.2.x.

This FortiOS Handbook chapter contains the following sections:

Packet flow describes the life of a packet as it passes through a FortiGate unit

Comparison of inspection types shows how different security functions map to different inspection types.

Client/Server connection packet flow example

Routing table update packet flow example

Dialup IPsec VPN with Application control example

Packet flow

After the FortiGate unit's external interface receives a packet, the packet proceeds through a number of steps on its way to the internal interface, traversing each of the inspection types, depending on the security policy and security profile configuration. The diagram below is a high level view of the packet's journey.

The description following is a high-level description of these steps as a packet enters the FortiGate unit towards its destination on the internal network. Similar steps occur for outbound traffic.

Packet flow consists of the following modules:

Ingress packet flow

- Interface TCP/IP stack
- DoS Sensor
- Interface policy
- IP integrity header checking
- IPsec VPN
- Destination NAT (DNAT)
- Routing

Stateful inspection

- Local Management Traffic
- Policy Lookup
- Session Tracking
- Session helpers
- SSL VPN
- User Authentication
- Traffic Shaping

Flow-based inspection

- IPS
- Application Control
- Web Filter
- DLP
- Antivirus

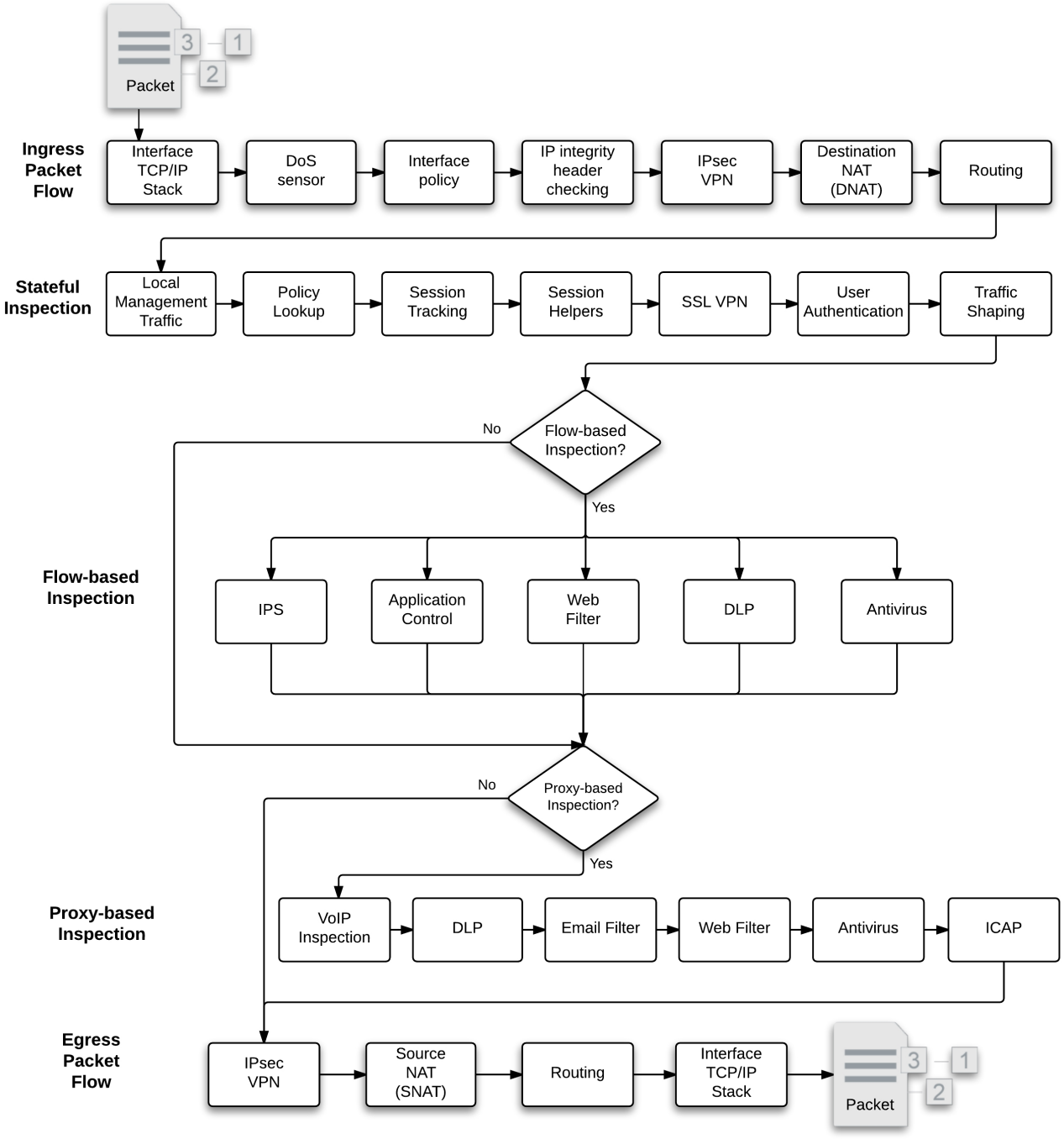
Proxy-based inspection

- VoIP Inspection
- DLP
- Email Filter
- Web Filter
- Antivirus
- ICAP

Egress packet flow

- IPsec VPN
- Source NAT (SNAT)
- Routing
- Interface TCP/IP stack

High-level Packet flow diagram



Ingress packet flow

When a packet is received by an interface and enters a FortiGate the following steps occur:

Interface TCP/IP stack

Ingress packets are received by a FortiGate interface.The packet enters the system, and the interface network device driver passes the packet to the Denial of Service (DoS) sensors, if enabled, to determine whether this is a valid information request or not.

DoS sensor

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack.The DoS module inspects all traffic flows but only tracks packets that can be used for DoS attacks (for example, TCP SYN packets), to ensure they are within the permitted parameters. Suspected DoS attacks are blocked, other packets are allowed.

IP integrity header checking

The FortiGate unit reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.

IPsec VPN

If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. If the IPsec engine can apply the correct encryption keys and decrypt the packet, the unencrypted packet is sent to the next step. Non-IPsec traffic and IPsec traffic that cannot be decrypted passes on to the next step without being affected.

Interface policy

Interface policies apply flow-based inspection to packets received at an interface before the packets are accepted by a firewall policy. Interface policies can also be applied decrypted IPsec VPN traffic. Using interface policies you can apply IPS sensors, application control and flow-based web filtering and virus scanning to traffic before it is accepted by a firewall policy. Packets can be dropped or alowed depending on the sensor or profile settings.

Destination NAT (DNAT)

The FortiGate unit checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. DNAT is typically applied to traffic from the Internet that is going to be directed to a server on a network behind the FortiGate. DNAT means the actual address of the internal network is hidden from the Internet. This step determines whether a route to the destination address actually exists.

DNAT must take place before routing so that the FortiGate unit can route packets to the correct destination.

Routing

The routing step uses the routing table to determine the interface to be used by the packet as it leaves the FortiGate unit. Routing also distinguishes between local traffic and forwarded traffic. Firewall policies are matched with packets depending on the source and destination interface used by the packet. The source interface is known when the packet is received and the destination interface is determined by routing.

Stateful inspection

Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed.

When the first packet is a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).

Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way.

When the final packet in the session is processed, the session is removed from the session table. Stateful inspection also has a session idle timeout that removes sessions from the session table that have been idle for the length of the timeout.

See the Stateful Firewall Wikipedia article (https://en.wikipedia.org/wiki/Stateful_firewall) for an excellent descruption of stateful inspection.

Local management traffic

Local management traffic terminates at a FortiGate interface. This can be any FortiGate interface included dedicated management interfaces. In multiuple VDOM mode local management traffic terminates at the management interface. In Transparent mode, local management traffic terminates at the management IP address.

Local management traffic includes administrative access, some routing protocol communication, central management from FortiManager, communication with the FortiGuard network and so on. Management traffic is allowed or blocked according to the Local In Policy list which lists all management protocols and their access control settings. You configure local management access indirectly by configuring administrative access and so on.

Management traffic is processed by applications such as the web server which displays the FortiOS web-based manager, the SSH server for the CLI or the FortiGuard server to handle local FortiGuard database updates or FortiGuard Web Filtering URL lookups.

Local management traffic is not involved in subsequent stateful inspection steps.

SSL VPN traffic terminates at a FortiGate interface similar to local management traffic. However, SSL VPN traffic uses a different destination port number that administrative traffic and can thus be detected and handled differently.

Policy lookup

The first stateful inspection step is a policy lookup that matches the packet with a firewall policy based on standard firewall matching criteria (source and destination interfaces, source and destination IP addresses, and port numbers). If the policy denies the packet it is discarded. An accepted packet continues to the next step.

Many FortiOS features are applied to traffic depending on the settings in the policy that matches the traffic as determined by the policy lookup. This includes authentication, security features and so on.

Session tracking

As described above for stateful inspection. Sessions are tracked in a session table after policy lookup has identified a new session.

Session helpers

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall. FortiOS includes the following session helpers:

- PPTP
- H323
- RAS
- TNS
- TFTP
- RTSP
- FTP
- MMS
- PMAP
- SIP
- DNS-UDP
- RSH
- DCERPC
- MGCP

SSL VPN

Local SSL VPN traffic is treated like special management traffic as determined by the SSL VPN destination port. Packets are decrypted and are routed to an SSL VPN interface. Polcy lookup is then used to control how packets are forwarded to their destination outside the FortiGate.

User Authentication

User authentication added to security policies is handled by the stateful inspection, which is why Firewall authentication is based on IP address. Authentication takes place after policy lookup selects a policy that includes authentication.

Traffic Shaping

If the policy that matches the packet includes traffic shaping it is applied as the last stateful inspection step.

Flow-based inspection

Flow-based inspection identifies and blocks security threats in real time as they are identified.

Flow-based inspection samples packets in a session and uses single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats. Depending on the options selected in the firewall policy that

accepted the session, flow-based inspection can apply **IPS**, **Application Control**, **Web Filtering**, **DLP** and **Antivirus**.

All of the applicable flow-based security modules are applied simultaneously in one pass. IPS, Application Control, Web Filtering and DLP filtering happen together. Flow-based antivirus caches files during protocol decoding and submits cached files for virus scanning while the other matching is carried out.

Flow inspection typically requires less processing resources than proxy inspection and since its not a proxy, flow-based inspection does not change packets (unless a threat is found and packets are blocked). Flow-based inspection cannot apply as many features as proxy inspection (for example, flow-based inspection does not support client comforting and some aspects of replacement messages).

IPS and Application Control are only applied using flow-based inspection. Web Filtering, DLP and Antivirus can also be applied using proxy-based inspection.

Proxy-based inspection

Proxy-based inspection uses a proxy to inspect content traffic (VoIP, HTTP, HTTPS, FTP, email, and others) for threats. The proxy extracts and caches content, such as files and web pages, from a content session and inspects the cached content for threats. Content inspection happens in the following order: **VoIP inspection**, **DLP**, **Email Filtering**, **Web Filtering**, **Antivirus**, and **ICAP**. If no threat is found the proxy relays the content to its destination. If a threat is found the proxy can block the content and replace it with a replacement message.

The proxy can also block VoIP traffic that contains threats. VoIP inspection can also look inside VoIP packets and extract port and address information and open pinholes in the firewall to allow VoIP traffic through.

ICAP intercepts HTTP and HTTPS traffic and forwards it to an ICAP server. The FortiGate unit is the surrogate, or “middle-man”, and carries the ICAP responses from the ICAP server to the ICAP client; the ICAP client then responds back, and the FortiGate unit determines the action that should be taken with these ICAP responses and requests.

Egress packet flow

After stateful inspection and flow or proxy-based inspection the packet goes through the following steps before exiting.

IPsec VPN

If the packet is to be sent out an IPsec tunnel, it is at this stage the encryption and required encapsulation is performed.

Source NAT (SNAT)

The FortiGate unit checks the NAT table and determines if the source IP address for outgoing traffic must be changed using SNAT. SNAT is typically applied to traffic from an internal netwotk heading out to the Internet. SNAT means the actual address of the internal network is hidden from the Internet.

DNAT must take place before routing so that the FortiGate unit can route the packet to the correct destination.

Routing

The final routing step determines the next hop router to send the packet to after it exits the FortiGate unit.

Interface TCP/IP Stack

Egress packets are received by the interface network device driver which forwards the packet out the interface an onto the network.

Comparison of inspection types

The tables in this section show how different security functions map to different inspection types.

Mapping security functions to inspection types

The table below lists FortiOS security functions and shows whether they are applied during stateful inspection, flow-based inspection or proxy-based inspection.

FortiOS security functions and inspection types

Security Function	Stateful Inspection	Flow-based inspection	Proxy-based inspection
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
IPS		yes	
Antivirus		yes	yes
Application Control		yes	
Web filtering		yes	yes
DLP		yes	yes
Email Filtering			yes
VoIP inspection			yes
ICAP			yes

More informaion about inspection methods

The three inspection methods each have their own strengths and weaknesses. The following table looks at all three methods side-by-side.

Inspection methods comparison

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets	complete content
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best
Authentication	yes		
IPsec and SSL VPN	yes		
Antivirus protection		yes	yes
Web Filtering		yes	yes
Data Leak Protection (DLP)		yes	yes
Application control		yes	
IPS		yes	
Delay in traffic	minor	no	small
Reconstruct entire content		no	yes

Client/Server connection packet flow example

The following example illustrates the flow of a packet that is part of a session between a client and a web server with authentication, FortiGuard Web Filtering and antivirus.

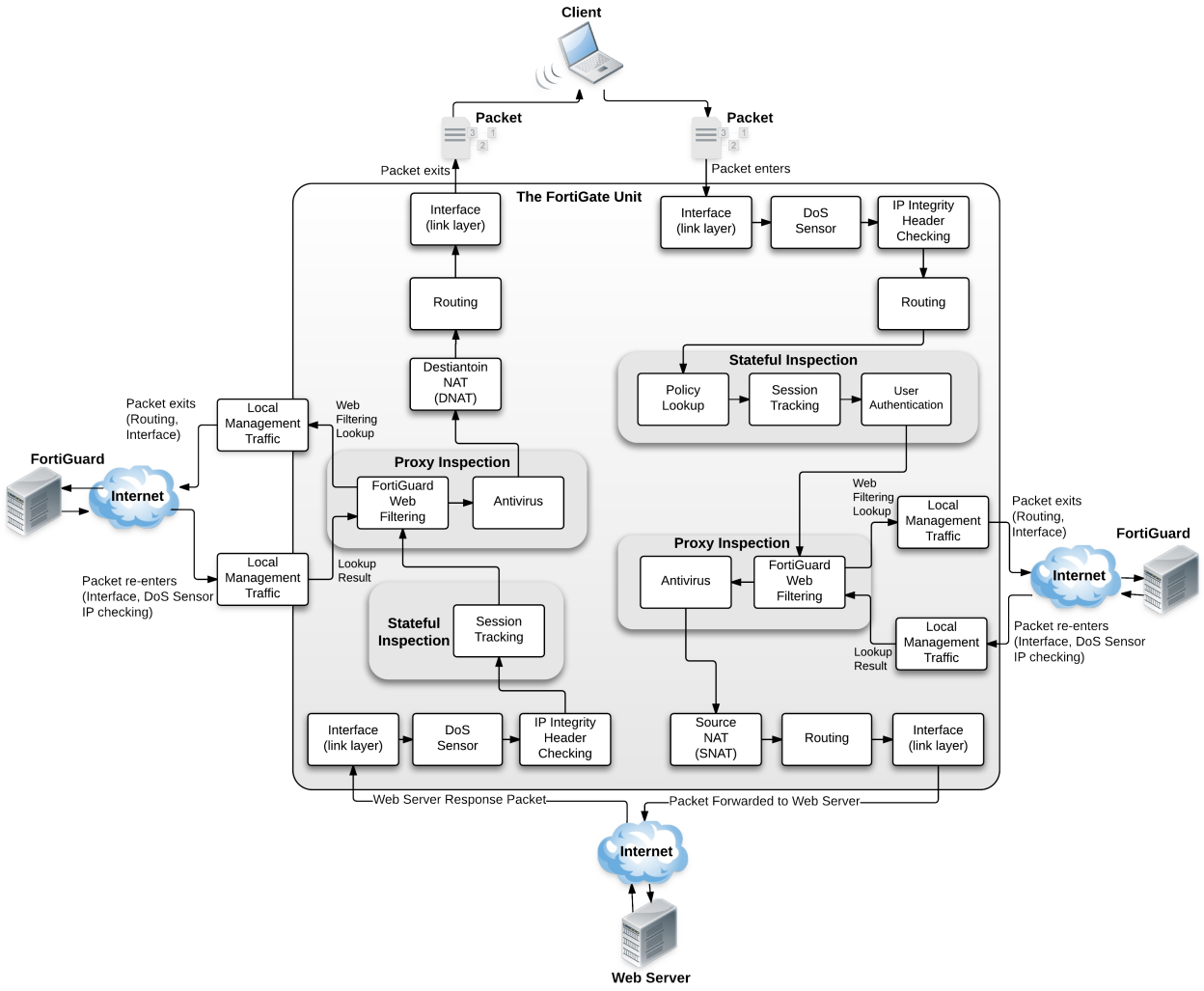
Initiating connection from client to web server

1. Client sends packet to web server.
2. The packed is routed to a FortiGate interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Routing.
6. Policy lookup.
7. User authentication.
8. Proxy-based inspection:
   - FortiGuard Web Filtering (FortiGuard web filtering lookup)
   - Antivirus
9. Source NAT changes the source address to the FortiGate IP address.
10. Routing.
11. Interface transmission to network.
12. Packet forwarded to web server.

Response from web server

1. Web Server sends response packet to client.
2. The packed is routed to a FortiGate interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Stateful inspection recognizes the packet is part and an established session.
6. Source NAT changes the destination address from the FortiGate interface back to the client IP address
7. Proxy-based inspection:
   - FortiGuard Web Filtering (FortiGuard Web Filtering lookup)
   - Antivirus
8. Packet is routed to the client.
9. Interface transmission to network
10. Packet returns to client

Life of a packet - Client/server connection



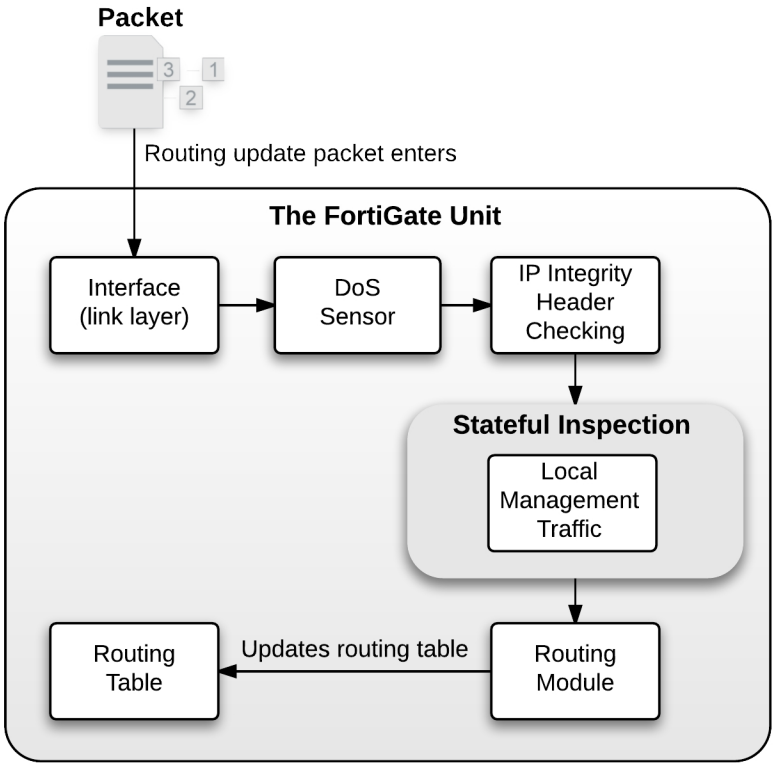
Routing table update packet flow example

The following example illustrates the flow of a packet when there is a routing table update. As this is low level, there is no security involved. This example includes the following steps:

1. FortiGate unit receives routing update packet
2. Packet intercepted by FortiGate unit interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Stateful policy engine
   Local Management traffic
6. Routing module
   Update routing table

The figure below illustrates the process steps.

Life of a Packet - Routing table update



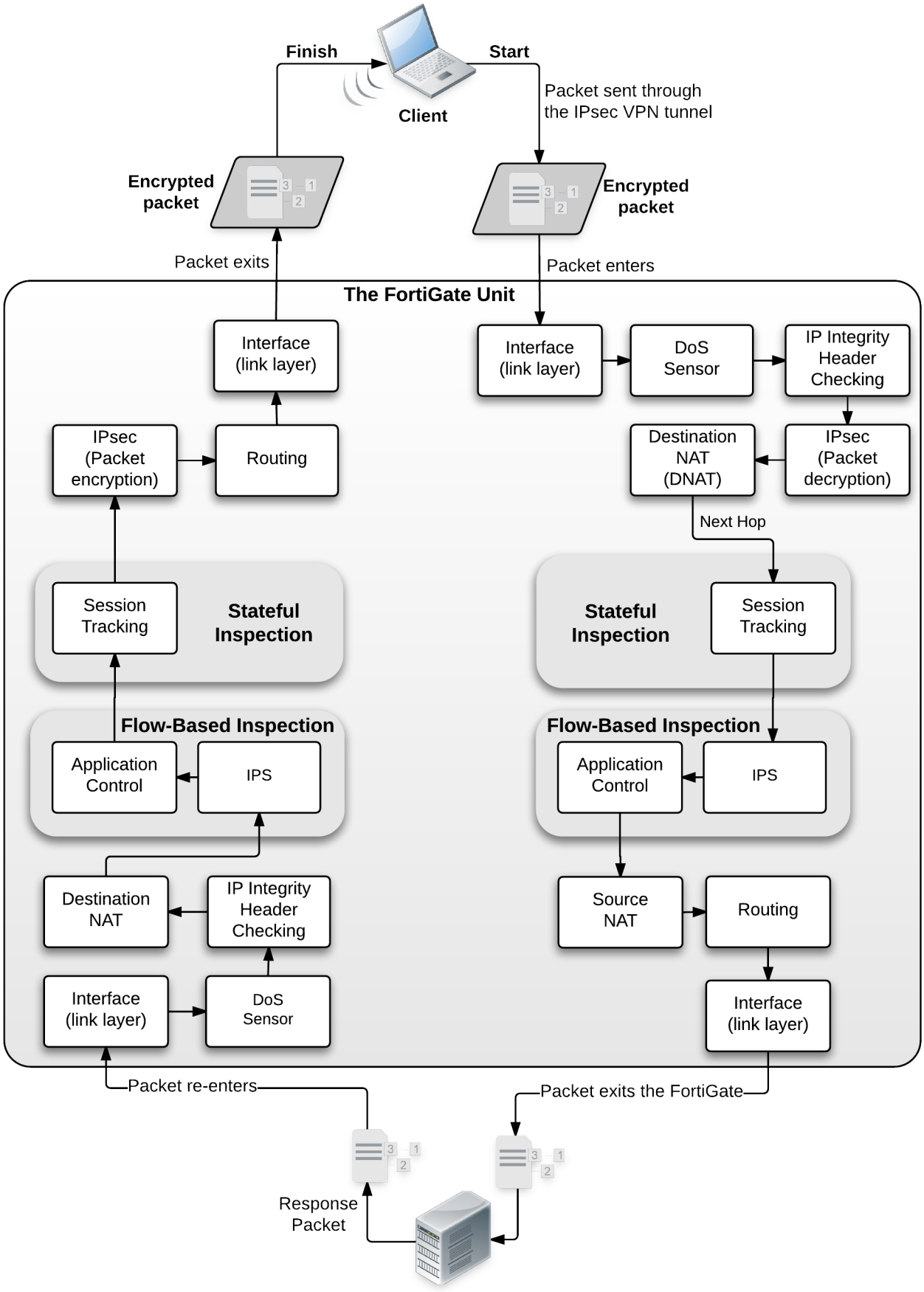
Dialup IPsec VPN with Application control example

This example includes these steps:

1. FortiGate unit receives IPsec encrypted packet from the Internet.
2. Packet intercepted by FortiGate unit interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. IPsec
   - Packet matches IPsec phase 1
   - Packet is unencrypted
6. Interface policy
7. Destination NAT
8. Next hop route
9. Stateful Inspection
   - Session Tracking
9. Flow-based inspection
   - IPS
   - Application Control
10. Source NAT
11. Routing
12. Interface transmission to network
13. Packet forwarded to internal server

Response from server

1. Server sends response packet
2. Packet intercepted by FortiGate unit interface
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Destination NAT
6. Flow-based inspection
   - IPS
   - Application Control
7. Stateful Inspection
   - Session Tracking
8. IPsec
   - Packet is encrypted
9. Routing
10. Interface transmission to network
11. Encrypted Packet returns to internet


Finish
Start
Client
Packet sent through the IPsec VPN tunnel
Encrypted packet
Encrypted packet
Packet exits
Packet enters
The FortiGate Unit
Interface (link layer)
Interface (link layer)
DoS Sensor
IP Integrity Header Checking
IPsec (Packet encryption)
Routing
Destination NAT (DNAT)
IPsec (Packet decryption)
Next Hop
Session Tracking
Stateful Inspection
Stateful Inspection
Session Tracking
Flow-Based Inspection
Application Control
IPS
Flow-Based Inspection
Application Control
IPS
Destination NAT
IP Integrity Header Checking
Source NAT
Routing
Interface (link layer)
DoS Sensor
Interface (link layer)
Packet re-enters
Packet exits the FortiGate
Response Packet
Internal Server

Chapter 17 - Load Balancing

FortiOS server load balancing includes the features you would expect of any server load balancing solution. Traffic can be distributed across multiple backend servers based on multiple methods including static (failover), round robin, weighted to account for different sized servers, or based on the health and performance of the server including round trip time, number of connections. The load balancer supports HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL or generic TCP/UDP or IP protocols. Session persistence is supported based on the SSL session ID or based on an injected HTTP cookie.

Before you begin

Before you begin to configure load balancing from the web-based manager you should go to **System > Config > Features** and turn on **Load Balancing**. To find Load Balancing select the **Show More** button.

How this chapter is organized

This document contains detailed information about how to configure firewall server load balancing to load balance various types of traffic to multiple backend servers. This document describes all server load balancing configuration options and contains detailed configuration examples.

This FortiOS Handbook chapter contains the following sections:

Configuring load balancing describes FortiOS server load balancing.

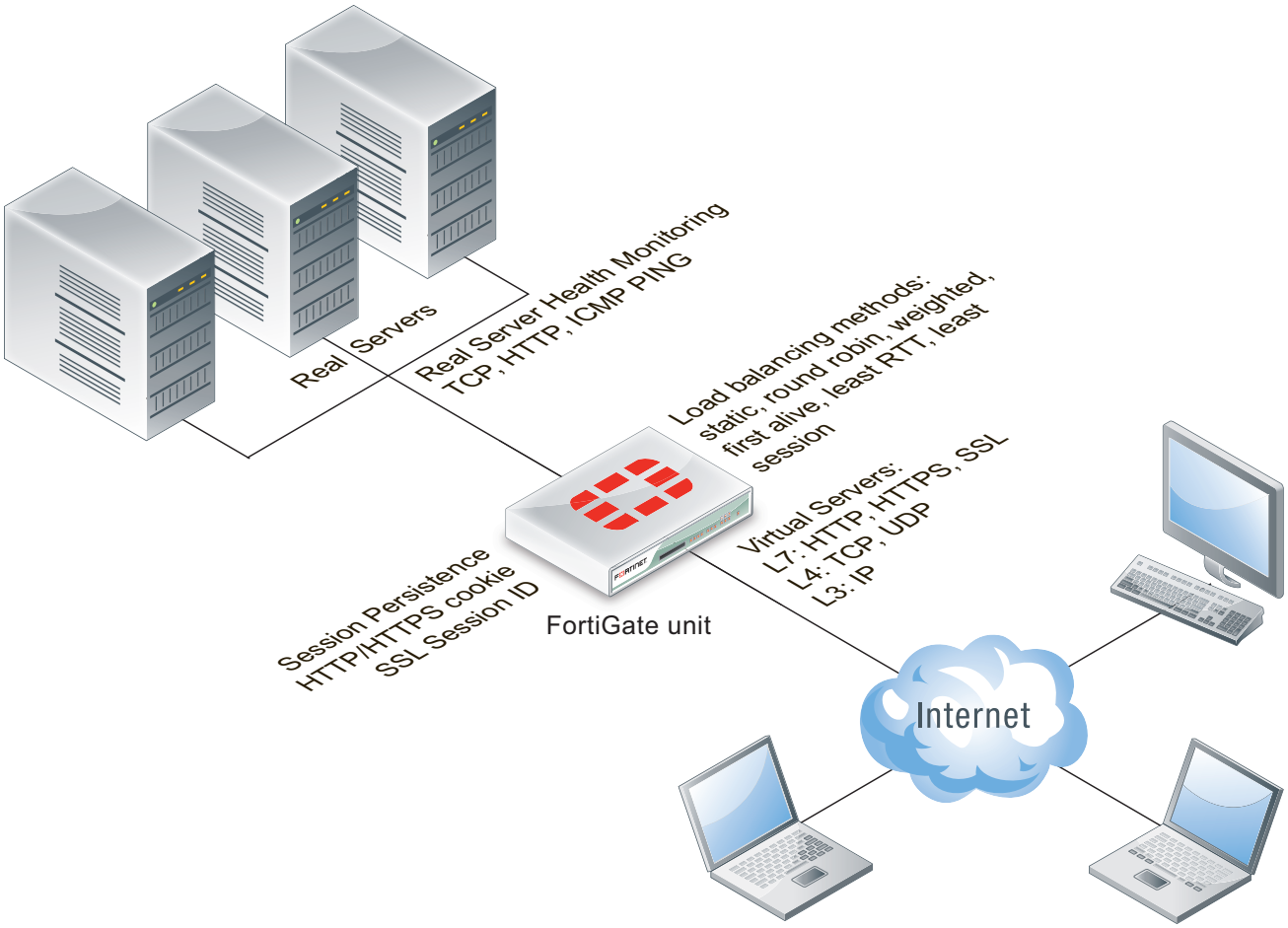
Load balancing configuration examples describes some basic and advanced load balancing configurations.

Configuring load balancing

This section describes how to use the FortiOS server load balancing to load balance traffic to multiple backend servers.

You can configure FortiOS load balancing to intercept incoming traffic with a virtual server and distribute it among one or more backend real servers. By doing so, FortiOS enables multiple real servers to respond as if they were a single device or virtual server. This in turn means that more simultaneous requests can be handled by the servers.

Server load balancing configuration



Traffic can be balanced across multiple backend real servers based on a selection of load balancing methods including static (failover), round robin, weighted to account for different sized servers, or based on the health and performance of the server including round trip time, number of connections. The load balancer can balance layer 7 HTTP, HTTPS, SSL, generic layer 4 TCP, UDP and generic layer 3 IP protocols. Session persistence is supported based on injected HTTP/HTTPS cookies or the SSL session ID.

You can bind up to 8 real servers can to one virtual server. The real server topology is transparent to end users, and the users interact with the system as if it were only a single server with the IP address and port number of the virtual server. The real servers may be interconnected by high-speed LAN or by geographically dispersed WAN.

The FortiGate unit schedules requests to the real servers and makes parallel services of the virtual server to appear to involve a single IP address.

There are additional benefits to load balancing. First, because the load is distributed across multiple servers, the service being provided can be highly available. If one of the servers breaks down, the load can still be handled by the other servers. Secondly, this increases scalability. If the load increases substantially, more servers can be added behind the FortiGate unit in order to cope with the increased load.

Load balancing and other FortiOS features

Flow-based and proxy-based security features such as virus scanning, IPS, DLP, application control, and web filtering can be applied to load balanced sessions. This includes SSL offloading and multiplexing. Applying these UTM features to load balancing traffic may reduce load balancing performance.

Authentication is not supported for load balancing sessions. Usually FortiGate load balancing is used to allow public access to services on servers protected by a FortiGate unit. Authentication is not generally not required for this kind of configuration.

Features such web proxying, web caching, and WAN optimization also do not work with load balanced sessions. However, most other features that can be applied by a security policy are supported.

Configuring load balancing from the web-based manager

A virtual server is a specialized firewall virtual IP that performs server load balancing. From the web-based manager you add load balancing virtual server by going to **Policy & Objects > Load Balance > Virtual Servers**.

Name

Enter the name for the virtual server.

Type

Select the protocol to be load balanced by the virtual server. If you select a general protocol such as **IP**, **TCP**, or **UDP** the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as **HTTP**, **HTTPS**, or **SSL** you can apply additional server load balancing features such as **Persistence** and **HTTP Multiplexing**.

- Select **HTTP** to load balance only HTTP sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can also select **HTTP Multiplex**. You can also set **Persistence** to **HTTP Cookie** to select cookie-based persistence.
- Select **HTTPS** to load balance only HTTPS sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can also select **Multiplex HTTP requests/responses.** You can also set **Persistence** to **HTTP Cookie** to select cookie-based persistence. You can also set **Persistence** to **SSL Session ID**.
- Select **IMAPS** to load balance only IMAPS sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced (usually port 993 for IMAPS sessions). You can also set **Persistence** to **SSL Session ID**.

- Select **POP3S** to load balance only POP3S sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced (usually port 995 for POP3S sessions). You can also set **Persistence** to **SSL Session ID**.
- Select **SMTPS** to load balance only SMTPS sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced (usually port 465 for SMTPS sessions). You can also set **Persistence** to **SSL Session ID**.
- Select **SSL** to load balance only SSL sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced.
- Select **TCP** to load balance only TCP sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced.
- Select **UDP** to load balance only UDP sessions with destination port number that matches the **Virtual Server Port** setting. Change **Virtual Server Port** to match the destination port of the sessions to be load balanced.
- Select **IP** to load balance all sessions accepted by the security policy that contains this virtual server.

Interface

Select the virtual server external interface from the list. The external interface is connected to the source network and receives the packets to be forwarded to the destination network.

Virtual Server IP

The IP address of the virtual server. This is an IP address on the external interface that you want to map to an address on the destination network.

Virtual Server Port

Enter the external port number that you want to map to a port number on the destination network. Sessions with this destination port are load balanced by this virtual server.

Load Balance Method

Select the load balancing method used by the virtual server.

Persistence

Configure persistence to make sure that a user is connected to the same server every time they make a request that is part of the same session. Session persistence is supported for HTTP and SSL sessions.

HTTP Multiplexing

Select to use the FortiGate unit to multiplex multiple client connections into a few connections between the FortiGate unit and the real server.

Preserve Client IP

Select to preserve the IP address of the client in the `X-Forwarded-For` HTTP header. This can be useful if you want log messages on the real servers to the client's original IP address. If this option is not selected, the header will contain the IP address of the FortiGate unit.

This option appears only if **HTTP** or **HTTS** are selected for **Type**, and is available only if **HTTP Multiplexing** is selected.

SSL Offloading

Select to accelerate clients' SSL connections to the server by using the Fortinet FortiGate unit to perform SSL operations, then select which segments of the connection will receive SSL offloading.

Certificate

Select the certificate to use with **SSL Offloading**. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

This option appears only if **HTTPS** or **SSL** are selected for **Type**, and is available only if **SSL Offloading** is selected.

Health Check

Select which health check monitor configuration will be used to determine a server's connectivity status.

Configuring load balancing from the CLI

From the CLI you configure load balancing by adding a firewall virtual IP and setting the virtual IP type to server load balance:

```
config firewall vip
   edit Vserver-HTTP-1
      set type server-load-balance
      ...
```

A virtual server includes a virtual server IP address bound to an interface. The virtual server IP address is the destination address incoming packets to be load balanced and the virtual server is bound to the interface that receives the packets to be load balanced.

For example, if you want to load balance incoming HTTP traffic from the Internet to a group of web servers on a DMZ network, the virtual server IP address is the known Internet IP address of the web servers and the virtual server binds this IP address to the FortiGate interface connected to the Internet.

When you bind the virtual server's external IP address to a FortiGate unit interface, by default, the network interface responds to ARP requests for the bound IP address. Virtual servers use proxy ARP, as defined in RFC 1027, so that the FortiGate unit can respond to ARP requests on a network for a real server that is actually installed on another network. In some cases you may not want the network interface sending ARP replies. You can use the `arp-reply` option disable sending ARP replies:

```
config firewall vip
   edit Vserver-HTTP-1
      set type server-load-balance
      set arp-reply disable
      ...
```

The load balancing virtual server configuration also includes the virtual server port. This is the TCP port on the bound interface that the virtual server listens for traffic to be load balanced on. The virtual server can listen on any port.

Load balancing methods

The load balancing method defines how sessions are load balanced to real servers. A number of load balancing methods are available as listed below.

All load balancing methods will not send traffic to real servers that are down or not responding. However, the FortiGate unit can only determine if a real server is not responding by using a health check monitor. You should always add at least one health check monitor to a virtual server or to individual real servers, or load balancing methods may attempt to distribute sessions to real servers that are not functioning.

Source IP Hash

The traffic load is statically spread evenly across all real servers. However, sessions are not assigned according to how busy individual real servers are. This load balancing method provides some persistence because all sessions from the same source address always go to the same real server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed and persistence could be lost.

Round Robin

Directs new requests to the next real server, and treats all real servers as equals regardless of response time or number of connections. Dead real servers or non responsive real servers are avoided.

Weighted

Real servers with a higher weight value receive a larger percentage of connections. Set the real server weight when adding a real server.

First Alive

Always directs sessions to the first alive real server. This load balancing schedule provides real server failover protection by sending all sessions to the first alive real server and if that real server fails, sending all sessions to the next alive real server. Sessions are not distributed to all real servers so all sessions are processed by the “first” real server only.

First refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then all sessions always go to A as long as it is alive. If A goes down then sessions go to B and if B goes down sessions go to C. If A comes back up sessions go back to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers in the required order.

Least RTT

Directs sessions to the real server with the least round trip time. The round trip time is determined by a Ping health check monitor and is defaulted to 0 if no Ping health check monitors are added to the virtual server.

Least Session

Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing all have similar capabilities. This load balancing method uses the FortiGate session table to track the number of sessions being processed by each real server. The FortiGate unit cannot detect the number of sessions actually being processed by a real server.

HTTP Host

Load balances HTTP host connections across multiple real servers using the host’s HTTP header to guide the connection to the correct real server.

Session persistence

Use persistence to make sure that a user is connected to the same real server every time they make an HTTP, HTTPS, or SSL request that is part of the same user session. For example, if you are load balancing HTTP and HTTPS sessions to a collection of eCommerce web servers, when a user is making a purchase they will be starting multiple sessions as they navigate the eCommerce site. In most cases all of the sessions started by this user during on eCommerce session should be processed by the same real server. Typically, the HTTP protocol keeps track of these related sessions using cookies. HTTP cookie persistence makes sure that all sessions that are part of the same user session are processed by the same real server

When you configure persistence, the FortiGate unit load balances a new session to a real server according to the load balance method. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. For more information about HTTP and HTTPS persistence, see "HTTP and HTTPS persistence".

Real servers

Add real servers to a load balancing virtual server to provide the information the virtual server requires to be able to send sessions to the server. A real server configuration includes the IP address of the real server and port number that the real server receives sessions on. The FortiGate unit sends sessions to the real server's IP address using the destination port number in the real server configuration.

When configuring a real server you can also specify the weight (used if the load balance method is set to weighted) and you can limit the maximum number of open connections between the FortiGate unit and the real server. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests other real servers until the connection number drops below the specified limit. Setting Maximum Connections to 0 means that the FortiGate unit does not limit the number of connections to the real server.

Real server active, standby, and disabled modes

By default the real server mode setting is active indicating that the real server is available to receive connections. If the real server is removed from the network (for example, for routine maintenance or because of a hardware or software failure) you can change the mode to standby or disabled. In disabled mode the FortiGate unit no longer sends sessions to the real server.

If a real server is in standby mode the FortiGate also does not send sessions to it unless other real servers added to the same virtual server become unavailable. For example:

- A virtual server that includes two real servers one in active mode and one in standby mode. If the real server in active mode fails, the real server in standby mode is changed to active mode and all sessions are sent to this real server.
- A virtual server includes three real servers, two in active mode and one in standby mode, if one of the real servers in active mode fails, the real server in standby mode is changed to active mode and sessions are load balanced between it and still operating real server. If both real servers in active mode fail, all sessions are sent to the real server in standby mode.

Adding real servers from the web-based manager

To add a real server from the web-based manager go to **Policy & Objects > Load Balance > Real Servers**.

Virtual Server

Select the virtual server that will send sessions to this real server.

IP Address

Enter the IP address of the real server.

Port

Enter the port number on the destination network to which the external port number is mapped.

Weight

Enter the weight value of the real server. The higher the weight value, the higher the percentage of connections the server will handle. A range of 1-255 can be used. This option is available only if the associated virtual server's load balance method is **Weighted**.

Max Connections

Enter the limit on the number of active connections directed to a real server. A range of 1-99999 can be used. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests to another server until the connection number drops below the specified limit.

Setting **Maximum Connections** to **0** means that the FortiGate unit does not limit the number of connections to the real server.

HTTP Host

Enter the HTTP header for load balancing across multiple real servers. This feature is used for load balancing HTTP host connections across multiple real servers using the host's HTTP header to guide the connection to the correct real server, providing better load balancing for those specific connections.

Mode

Select a mode for the real server.

Adding real servers from the CLI

To add a real server from the CLI you configure a virtual server and add real servers to it. For example, to add three real servers to a virtual server that load balances UDP sessions on port 8190 using weighted load balancing. For each real server the port is not changed. The default real server port is 0 resulting in the traffic being sent the real server with destination port 8190. Each real sever is given a different weight. Servers with higher weights have a max-connections limit to prevent too many sessions from being sent to them.

```
config firewall vip
   edit Vserver-UDP-1
      set type server-load-balance
      set server-type udp
      set ldb-method weighted
      set extip 172.20.120.30
      set extintf wan1
      set extport 8190
```

```
    set monitor ping-mon-1
       config realservers
          edit 1
             set ip 10.31.101.30
             set weight 100
             set max-connections 10000
          next
          edit 2
             set ip 10.31.101.40
             set weight 100
             set max-connections 10000
          next
          edit 3
             set ip 10.31.101.50
             set weight 10
          end
end
```

Health check monitoring

From the FortiGate web-based manager you can go to **Policy & Objects > Load Balance > Health Check** and configure health check monitoring so that the FortiGate unit can verify that real servers are able respond to network connection attempts. If a real server responds to connection attempts the load balancer continues to send sessions to it. If a real server stops responding to connection attempts the load balancer assumes that the server is down and does not send sessions to it. The health check monitor configuration determines how the load balancer tests the real servers. You can use a single health check monitor for multiple load balancing configurations.

You can configure TCP, HTTP and Ping health check monitors. Usually you would want the health check monitor to use the same protocol for checking the health of the server as the traffic being load balanced to it. For example, for an HTTP load balancing configuration you would normally use an HTTP health check monitor.

For the TCP and HTTP health check monitors you can specify the destination port to use to connect to the real servers. If you set the port to 0, the health check monitor uses the port defined in the real server. This allows you to use the same health check monitor for multiple real servers using different ports. You can also configure the interval, timeout and retry. A health check occurs every number of seconds indicated by the interval. If a reply is not received within the timeout period the health check is repeated every second. If no response is received after the number of configured retires, the virtual server is considered unresponsive, and load balancing will disabling traffic to that real server. The health check monitor will continue to contact the real server and if successful, the load balancer can resume sending sessions to the recovered real server.

The default health check configuration has an interval of 10 seconds, a timeout of 2 seconds and a retry of 3. This means that the health check monitor checks the health of a real server every 10 seconds. If a reply is not received within 2 seconds the health check monitor re-checks the server every second for 3 retries. If no response is received for 2 seconds after the final retry the server is considered unresponsive. This entire process takes a total of 7 seconds to consider a virtual server as unresponsive (2 second timeout + (3 re-checks x 1 second) + 2 second timeout = 7 seconds). Since this health check process is repeated every 10 seconds, a server can be down for a maximum of 10 + 7 = 17 seconds before the health check monitor considers it down.

For HTTP health check monitors, you can add URL that the FortiGate unit connects to when sending a get request to check the health of a HTTP server. The URL should match an actual URL for the real HTTP servers. The URL is optional.

The URL would not usually include an IP address or domain name. Instead it should start with a "/" and be followed by the address of an actual web page on the real server. For example, if the IP address of the real server is 10.31.101.30, the URL "/test_page.htm" causes the FortiGate unit to send an HTTP get request to "http://10.31.101.30/test_page.htm".

For HTTP health check monitors, you can also add a matched content phrase that a real HTTP server should include in response to the get request sent by the FortiGate unit using the content of the URL option. If the URL returns a web page, the matched content should exactly match some of the text on the web page. You can use the URL and Matched Content options to verify that an HTTP server is actually operating correctly by responding to get requests with expected web pages. Matched content is only required if you add a URL.

For example, you can set matched content to "server test page" if the real HTTP server page defined by the URL option contains the phrase "server test page". When the FortiGate unit receives the web page in response to the URL get request, the system searches the content of the web page for the matched content phrase.

Name

Enter the name of the health check monitor configuration.

Type

Select the protocol used to perform the health check.

- TCP
- HTTP
- PING

Port

Enter the port number used to perform the health check. If you set the **Port** to 0, the health check monitor uses the port defined in the real server. This way you can use a single health check monitor for different real servers.

This option does not appear if the **Type** is **PING**.

Interval

Enter the number of seconds between each server health check.

URL

For HTTP health check monitors, add a URL that the FortiGate unit uses when sending a get request to check the health of a HTTP server. The URL should match an actual URL for the real HTTP servers. The URL is optional.

The URL would not usually include an IP address or domain name. Instead it should start with a "/" and be followed by the address of an actual web page on the real server. For example, if the IP address of the real server is 10.10.10.1, the **URL** "/test_page.htm" causes the FortiGate unit to send an HTTP get request to "http://10.10.10.1/test_page.htm".

This option appears only if **Type** is **HTTP**.

Matched Content

For HTTP health check monitors, add a phrase that a real HTTP server should include in response to the get request sent by the FortiGate unit using the content of the **URL** option. If the **URL** returns a web page, the **Matched Content** should exactly match some of the text on the web page. You can use the **URL** and **Matched**

Content options to verify that an HTTP server is actually operating correctly by responding to get requests with expected web pages. Matched content is only required if you add a URL.

For example, you can set **Matched Content** to “server test page” if the real HTTP server page defined by the URL option contains the phrase “server test page”. When the FortiGate unit receives the web page in response to the URL get request, the system searches the content of the web page for the **Matched Content** phrase.

This option appears only if **Type** is **HTTP**.

Timeout

Enter the number of seconds which must pass after the server health check to indicate a failed health check.

Retry

Enter the number of times, if any, a failed health check will be retried before the server is determined to be inaccessible.

Load balancing limitations

The following limitations apply when adding virtual IPs, load balancing virtual servers, and load balancing real servers. Load balancing virtual servers are actually server load balancing virtual IPs. You can add server load balance virtual IPs from the CLI.

- Virtual IP **External IP Address/Range** entries or ranges cannot overlap with each other or with load balancing virtual server **Virtual Server IP** entries.
- A virtual IP **Mapped IP Address/Range** cannot be 0.0.0.0 or 255.255.255.255.
- A real server **IP** cannot be 0.0.0.0 or 255.255.255.255.
- If a static NAT virtual IP **External IP Address/Range** is 0.0.0.0, the **Mapped IP Address/Range** must be a single IP address.
- If a load balance virtual IP **External IP Address/Range** is 0.0.0.0, the **Mapped IP Address/Range** can be an address range.
- When port forwarding, the count of mapped port numbers and external port numbers must be the same. The web-based manager does this automatically but the CLI does not.
- Virtual IP and virtual server names must be different from firewall address or address group names.

Monitoring load balancing

From the web-based manager you can go to **Policy & Objects > Monitor > Load Balance Monitor** to monitor the status of configured virtual servers and real server and start or stop the real servers. You can also use the `get test ipldb` command from the CLI to display similar information.

For each real server the monitor displays health status (up or down), active sessions, round trip time and the amount of bytes of data processed. From the monitor page you can also stop sending new sessions to any real server. When you select to stop sending sessions the FortiGate unit performs of graceful stop by continuing to send data for sessions that were established or persistent before you selected stop. However, no new sessions are started.

Virtual Server

The IP addresses of the existing virtual servers.

Real Server

The IP addresses of the existing real servers.

Health Status

Displays the health status according to the health check results for each real server. A green arrow means the server is up. A red arrow means the server is down.

Mode

The mode of the health check monitor. Can be active, standby, or disabled.

Monitor Events

Display each real server's up and down times.

Active Sessions

Display each real server's active sessions.

RTT (ms)

Displays the Round Trip TIme (RTT) of each real server. By default, the RTT is "<1". This value will change only when ping monitoring is enabled on a real server.

Bytes Processed

Displays the traffic processed by each real server.

Graceful Stop/Start

Select to start or stop real servers. When stopping a server, the FortiGate unit will not accept new sessions but will wait for the active sessions to finish.

Load balancing diagnose commands

You can also use the following diagnose commands to view status information for load balancing virtual servers and real servers:

```
diagnose firewall vip realserver {down | flush | healthcheck | list | up}
diagnose firewall vip virtual-server {filter | log | real-server | session | stats}
```

For example, the following command lists and displays status information for all real servers:

```
diagnose firewall vip virtual-server real-server

vd root/0 vs vs/2 addr 10.31.101.30:80 status 1/1
conn: max 0 active 0 attempts 0 success 0 drop 0 fail 0

vd root/0 vs vs/2 addr 10.31.101.20:80 status 1/1
conn: max 0 active 0 attempts 0 success 0 drop 0 fail 0
```

Many of the diagnostic commands involve retrieving information about one or more virtual servers. To control which servers are queried you can define a filter:

```
diagnose firewall vip virtual-server filter <filter_str>
```

Where <filter_str> can be:

- clear erase the current filter
- dst the destination address range to filter by
- dst-port the destination port range to filter by
- list display the current filter
- name the vip name to filter by
- negate negate the specified filter parameter
- src the source address range to filter by
- src-port the source port range to filter by
- vd index of virtual domain. -1 matches all

The default filter is empty so no filtering is done.

Logging Diagnostics

The logging diagnostics provide information about two separate features:

```
diagnose firewall vip virtual-server log {console | filter}
```

Where

- console {disable | enable} enables or disables displaying the event log messages generated by virtual server traffic on the console to simplify debugging.
- filter sets a filter for the virtual server debug log
- The filter option controls what entries the virtual server daemon will log to the console if diagnose debug application vs level is non-zero. The filtering can be done on source, destination, virtual-server name, virtual domain, and so on:

```
diagnose firewall vip virtual-server log filter <filter_str>
```

Where <filter_str> can be

- clear erase the current filter
- dst the destination address range to filter by
- dst-port the destination port range to filter by
- list display the current filter
- name the virtual-server name to filter by
- negate negate the specified filter parameter
- src the source address range to filter by
- src-port the source port range to filter by
- vd index of virtual domain. -1 matches all

The default filter is empty so no filtering is done.

Real server diagnostics

Enter the following command to list all the real servers:

```
diag firewall vip virtual-server real-server list
```

In the following example there is only one virtual server called slb and it has two real-servers:

```
diag firewall vip virtual-server server
vd root/0 vs slb/2 addr 172.16.67.191:80 status 1/1
conn: max 10 active 0 attempts 0 success 0 drop 0 fail 0
http: available 0 total 0
```

```
vd root/0 vs slb/2 addr 172.16.67.192:80 status 1/1
conn: max 10 active 1 attempts 4 success 4 drop 0 fail 0
http: available 1 total 1
```

The `status` indicates the administrative and operational status of the real-server.

- `max` indicates that the real-server will only allow 10 concurrent connections.
- `active` is the number of current connections to the server attempts is the total number of connections attempted success is the total number of connections that were successful.
- `drop` is the total number of connections that were dropped because the active count hit max.
- `fail` is the total number of connections that failed to complete due to some internal problem (for example, lack of memory).

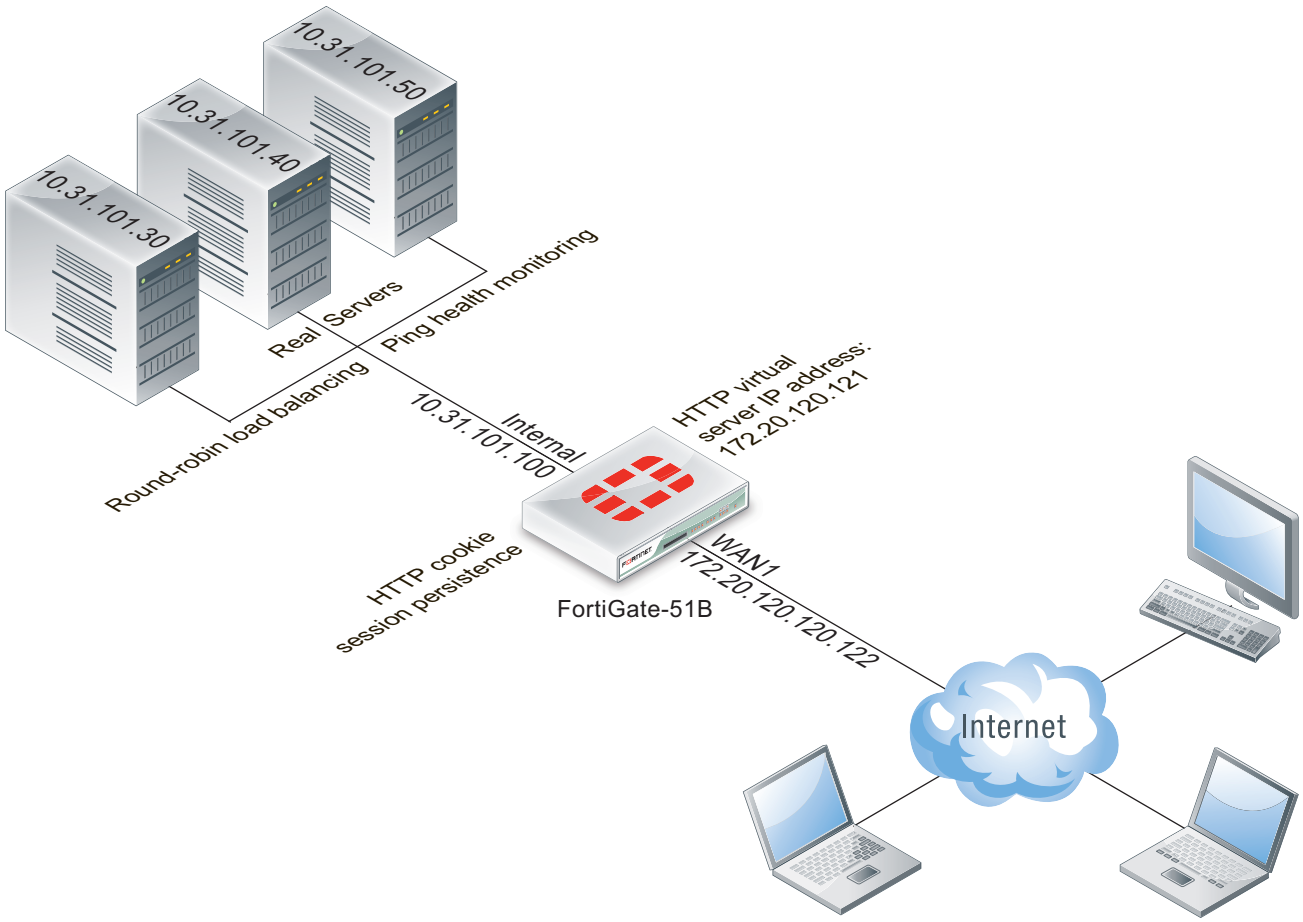
If the virtual server has HTTP multiplexing enabled then the HTTP section indicates how many established connections to the real-sever are available to service a HTTP request and also the total number of connections.

Basic load balancing configuration example

This section describes the steps required to configure the load balancing configuration shown below. In this configuration a FortiGate-51B unit is load balancing HTTP traffic from the Internet to three HTTP servers on the Internal network. HTTP sessions are accepted at the wan1 interface with destination IP address 172.20.120.121 on TCP port 8080 and forwarded from the internal interface to the web servers. When forwarded the destination address of the sessions is translated to the IP address of one of the web servers.

The load balancing configuration also includes session persistence using HTTP cookies, round-robin load balancing, and TCP health monitoring for the real servers. Ping health monitoring consists of the FortiGate unit using ICMP ping to make sure the web servers can respond to network traffic.

Virtual server and real servers setup



To configure the example load balancing configuration - general configuration steps

1. Add a load balance ping health check monitor.
   A ping health check monitor causes the FortiGate unit to ping the real servers every 10 seconds. If one of the servers does not respond within 2 seconds, the FortiGate unit will retry the ping 3 times before assuming that the HTTP server is not responding.
2. Add a load balance virtual server.
3. Add the three load balance real servers. Include the virtual server in each real server configuration.
4. Add a security policy that includes the load balance virtual server as the destination address.

To configure the example load balancing configuration - web-based manager

1. Go to **Policy & Objects > Load Balance > Health Check** and add the following health check monitor.

Name	Ping-mon-1
Type	Ping

Interval	10 seconds
Timeout	2 seconds
Retry	3

2. Go to **Policy & Objects > Load Balance > Virtual Servers** and add virtual server that accepts the traffic to be load balanced.

Name	Vserver-HTTP-1
Type	HTTP
Interface	wan1
Virtual Server IP	172.20.120.121
Virtual Server Port	8080
Load Balance Method	Round Robin
Persistence	HTTP Cookie
HTTP Multiplexing	Do not select
Health Check	Move Ping-mon-1 to the Selected list.

3. Go to **Policy & Objects > Load Balance > Real Servers** and add the real servers.

Virtual Server	Vserver-HTTP-1
IP Address	10.31.101.30
Port	80
Weight	n/a
Max Connections	0
Mode	Active

Virtual Server	Vserver-HTTP-1
IP Address	10.31.101.40
Port	80
Weight	n/a
Max Connections	0
Mode	Active

Virtual Server	Vserver-HTTP-1
IP Address	10.31.101.50
Port	80
Weight	n/a
Max Connections	0
Mode	Active

4. Go to **Policy & Objects > Policy > IPv4** and add a wan1 to internal security policy that includes the virtual server. This policy also applies an Antivirus profile to the load balanced sessions.

Incoming Interface	wan1
Source Address	all
Outgoing Interface	internal
Destination Address	Vserver-HTTP-1
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Turn on NAT and select **Use Destination Interface Address**.
Antivirus	Turn ON and select an Antivirus profile.

5. Select **OK**.

To configure the example load balancing configuration- CLI

1. Use the following command to add a Ping health check monitor.

```
config firewall ldb-monitor
   edit ping-mon-1
      set type ping
      set interval 10
      set timeout 2
      set retry 3
   end
```

2. Use the following command to add the virtual server that accepts HTTP sessions on port 8080 at the wan1 interface and load balances the traffic to three real servers.

```
config firewall vip
   edit Vserver-HTTP-1
      set type server-load-balance
      set server-type http
      set ldb-method round-robin
      set extip 172.20.120.30
      set extintf wan1
      set extport 8080
      set persistence http-cookie
```

```
      set monitor tcp-mon-1
         config realservers
            edit 1
               set ip 10.31.101.30
               set port 80
            next
            edit 2
               set ip 10.31.101.40
               set port 80
            end
end
```

3. Use the following command to add a security policy that includes the load balance virtual server as the destination address.

```
config firewall policy
   edit 0
      set srcintf wan1
      set srcaddr all
      set dstintf internal
      set dstaddr Vserver-HTTP-1
      set action accept
      set schedule always
      set service ALL
      set nat enable
      set utm-status enable
      set profile-protocol-options default
      set av-profile scan
   end
```

HTTP and HTTPS load balancing, multiplexing, and persistence

In a firewall load balancing virtual server configuration, you can select HTTP to load balance only HTTP sessions. The virtual server will load balance HTTP sessions received at the virtual server interface with destination IP address that matches the configured virtual server IP and destination port number that matches the configured virtual server port. The default virtual server port for HTTP load balancing is 80, but you can change this to any port number. Similarly for HTTPS load balancing, set the virtual server type to HTTPS and then select the interface, virtual server IP, and virtual server port that matches the HTTPS traffic to be load balanced. Usually HTTPS traffic uses port 443.

You can also configure load balancing to offload SSL processing for HTTPS and SSL traffic. See "SSL offloading" for more information.

HTTP and HTTPS multiplexing

For both HTTP and HTTPS load balancing you can multiplex HTTP requests and responses over a single TCP connection. HTTP multiplexing is a performance saving feature of HTTP/1.1 compliant web servers that provides the ability to pipeline many unrelated HTTP or HTTPS requests on the same connection. This allows a single HTTPD process on the server to interleave and serve multiple requests. The result is fewer idle sessions on the web server so server resources are used more efficiently. HTTP multiplexing can take multiple separate inbound sessions and multiplex them over the same internal session. This may reduce the load on the backend server and increase the overall performance.

HTTP multiplexing may improve performance in some cases. For example, if users web browsers are only compatible with HTTP 1.0. HTTP multiplexing can also improve performance between a web server and the

FortiGate unit if the FortiGate unit is performing SSL acceleration. However, in most cases HTTP multiplexing should only be used if enabling it leads to a measurable improvement in performance.

To enable HTTP multiplexing from the web-based manager, select multiplex HTTP requests/responses over a single TCP connection. To enable HTTP multiplexing from the CLI enable the `http-multiplex` option.

Preserving the client IP address

Select preserve client IP from the web-based manager or enable the `http-ip-header` option from the CLI to preserve the IP address of the client in the `X-Forwarded-For` HTTP header. This can be useful in an HTTP multiplexing configuration if you want log messages on the real servers to the client's original IP address. If this option is not selected, the header will contain the IP address of the FortiGate unit.

Preserving the client IP address but changing the X-Forwarded-For header name

If you select preserve client IP from the web-based manager or enable the `http-ip-header` option from the CLI you can also change the name of the `X-Forwarded-For` header to a custom header name. This can be useful if you want to use a custom header name instead of the standard header name.

You can configure changing the header name from the CLI. When `http-ip-header` is enabled you can add a custom header name to the `http-ip-header-name` option. If you don't add a custom header name the `X-Forwarded-For` header name is maintained.

HTTP and HTTPS persistence

Configure load balancing persistence for HTTP or HTTPS to make sure that a user is connected to the same server every time they make a request that is part of the same session. HTTP cookie persistence uses injected cookies to enable persistence.

When you configure persistence, the FortiGate unit load balances a new session to a real server according to the **Load Balance Method**. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server.

The following example shows how to enable cookie persistence and set the cookie domain to .example.org.

```
config firewall vip
   edit HTTP_Load_Balance
      set type server-load-balance
      set server-type http
      set extport 8080
      set extintf port2
      set extip 192.168.20.20
      set persistence http-cookie
      set http-cookie-domain .example.org
         config realservers
         edit 1
               set ip 10.10.10.1
               set port 80
         next
         edit 2
               set ip 10.10.10.2
               set port 80
         next
         edit 3
               set ip 10.10.10.3
               set port 80
```

```
    end
```

How HTTP cookie persistence options work

The following options are available for the `config firewall vip` command when `type` is set to `server-load-balance`, `server-type` is set to `http` or `https` and `persistence` is set to `http-cookie`:

```
http-cookie-domain-from-host
http-cookie-domain
http-cookie-path
http-cookie-generation
http-cookie-age
http-cookie-share
https-cookie-share
```

When HTTP cookie persistence is enabled the FortiGate unit inserts a header of the following form into each HTTP response unless the corresponding HTTP request already contains a `FGTServer` cookie:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1; Max-Age=3600
```

The value of the `FGTServer` cookie encodes the server that traffic should be directed to. The value is encoded so as to not leak information about the internal network.

Enable `http-cookie-domain-from-host` to extract the cookie domain from the `host:` header in the HTTP request. For example, to restrict the cookie to `.server.com`, enter:

The generated cookies could have the following form if the **Host:** header contains **exhost.com**:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
    Domain=.exhost.com; Max-Age=3600
```

For more information, see "HTTP host-based load balancing".

Use `http-cookie-domain` to restrict the domain that the cookie should apply to. For example, to restrict the cookie to `.server.com`, enter:

```
set http-cookie-domain .server.com
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
    Domain=.server.com; Max-Age=3600
```

Use `http-cookie-path` to limit the cookies to a particular path. For example, to limit cookies to the path `/sales`, enter:

```
set http-cookie-path /sales
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
    Domain=.server.com; Path=/sales; Max-Age=3600
```

Use `http-cookie-age` to change how long the browser caches the cookie. You can enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely:

```
set http-cookie-age 0
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
    Domain=.server.com; Path=/sales
```

Use `http-cookie-generation` to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used for cookies in this domain. The simplest approach is to increment the generation by one each time invalidation is required. Since the default is 0, enter the following to invalidate all existing cookies:

```
set http-cookie-generation 1
```

Use `http-cookie-share {disable | same-ip}` to control the sharing of cookies across virtual servers in the same virtual domain. The default setting `same-ip` means that any `FGTServer` cookie generated by one virtual server can be used by another virtual server in the same virtual domain. For example, if you have an application that starts on HTTP and then changes to HTTPS and you want to make sure that the same server is used for the HTTP and HTTPS traffic then you can create two virtual servers, one for port 80 (for HTTP) and one for port 443 (for HTTPS). As long as you add the same real servers to both of these virtual servers (and as long as both virtual servers have the same number of real servers with the same IP addresses), then cookies generated by accessing the HTTP server are reused when the application changes to the HTTPS server.

If for any reason you do not want this sharing to occur then select `disable` to make sure that a cookie generated for a virtual server cannot be used by other virtual servers.

Use `https-cookie-secure` to enable or disable using secure cookies. Secure cookies are disabled by default because secure cookies can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the `Secure` tag is added to the cookie inserted by the FortiGate unit:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1; Max-Age=3600;
    Secure
```

HTTP host-based load balancing

When configuring HTTP or HTTPS load balancing you can select HTTP host load balancing to load balances HTTP host connections across multiple real servers using the host's HTTP header to guide the connection to the correct real server. HTTP 1.1 includes the concept of a virtual server which allows a HTTP or HTTPS server with a single external IP address to serve requests for multiple DNS domains by using the mandatory `Host:` header in a HTTP request to indicate which DNS domain the request is destined for.

FortiOS can load-balance HTTP and HTTPS connections among multiple real servers using the `Host:` header to guide the connection to the correct real server. The host load balancing method allows a real server to specify a `http-host` attribute which is the domain name of the traffic for that real server. Each real server can only specify a single domain name. The same domain name can appear in more than one real server but only the first one that is up will be used, any others are purely for redundancy. If the Host: header contains a domain that does not match any http-host entry then the connection will be dropped. A real server with no http-host can be matched by any Host: domain.

For example, consider a FortiGate unit that is load-balancing traffic to three real servers. Traffic for www.example1.com should go to 192.168.2.1, traffic for www.example2.com should go to 192.168.2.2 and traffic to any other domain should go to 192.168.2.3. To enable this configuration you would add a virtual server and set the load balance method to HTTP host. Then you would add three real servers and set the HTTP host of the real server with IP address 192.168.2.1 to www.example1.com, the HTTP host of the real server with IP address 192.168.2.2 to www.example2.com and you would not specify an HTTP host for the third real server.

The configuration of a virtual IP to achieve this result would be:

```
config firewall vip
   edit "http-host-ldb"
      set type server-load-balance
      set extip 172.16.67.195
      set extintf "lan"
      set server-type http
      set ldb-method http-host
      set extport 80
         config realservers
         edit 1
               set http-host "www.example1.com"
```

```
            set ip 192.168.2.1
            set port 80
        next
        edit 2
            set http-host "www.example2.com"
            set ip 192.168.2.2
            set port 80
        next
        edit 3
            set ip 192.168.2.3
            set port 80
        next
        end
end
```

Host load balancing and HTTP cookie persistence

In an HTTP host-based load balancing configuration with HTTP cookie persistence enabled you can optionally configure cookie persistence to use the domain set in the host header as the cookie domain. You can do this by enabling the `http-cookie-domain-from-host` option, for example:

```
config firewall vip
   edit "http-host-ldb"
      set type server-load-balance
      set extip 172.16.67.195
      set extintf "lan"
      set server-type http
      set ldb-method http-host
      set extport 80
      set persistence http-cookie
      set http-cookie-domain-from-host enable
         config realservers
            edit 1
               set http-host "www.example1.com"
               set ip 192.168.2.1
               set port 80
            next
            edit 2
               set http-host "www.example2.com"
               set ip 192.168.2.2
               set port 80
            next
            edit 3
               set ip 192.168.2.3
               set port 80
            next
            end
end
```

SSL/TLS load balancing

In a firewall load balancing virtual server configuration, you can select SSL to load balance only SSL and TLS sessions. The virtual server will load balance SSL and TLS sessions received at the virtual server interface with destination IP address that matches the configured virtual server IP and destination port number that matches

the configured virtual server port. Change this port to match the destination port of the sessions to be load balanced.

For SSL load balancing you can also set persistence to SSL session ID. Persistence is achieved by the FortiGate unit sending all sessions with the same SSL session ID to the same real server. When you configure persistence, the FortiGate unit load balances a new session to a real server according to the **Load Balance Method**. If the session has an SSL session ID, the FortiGate unit sends all subsequent sessions with the same SSL session ID to the same real server.

SSL offloading

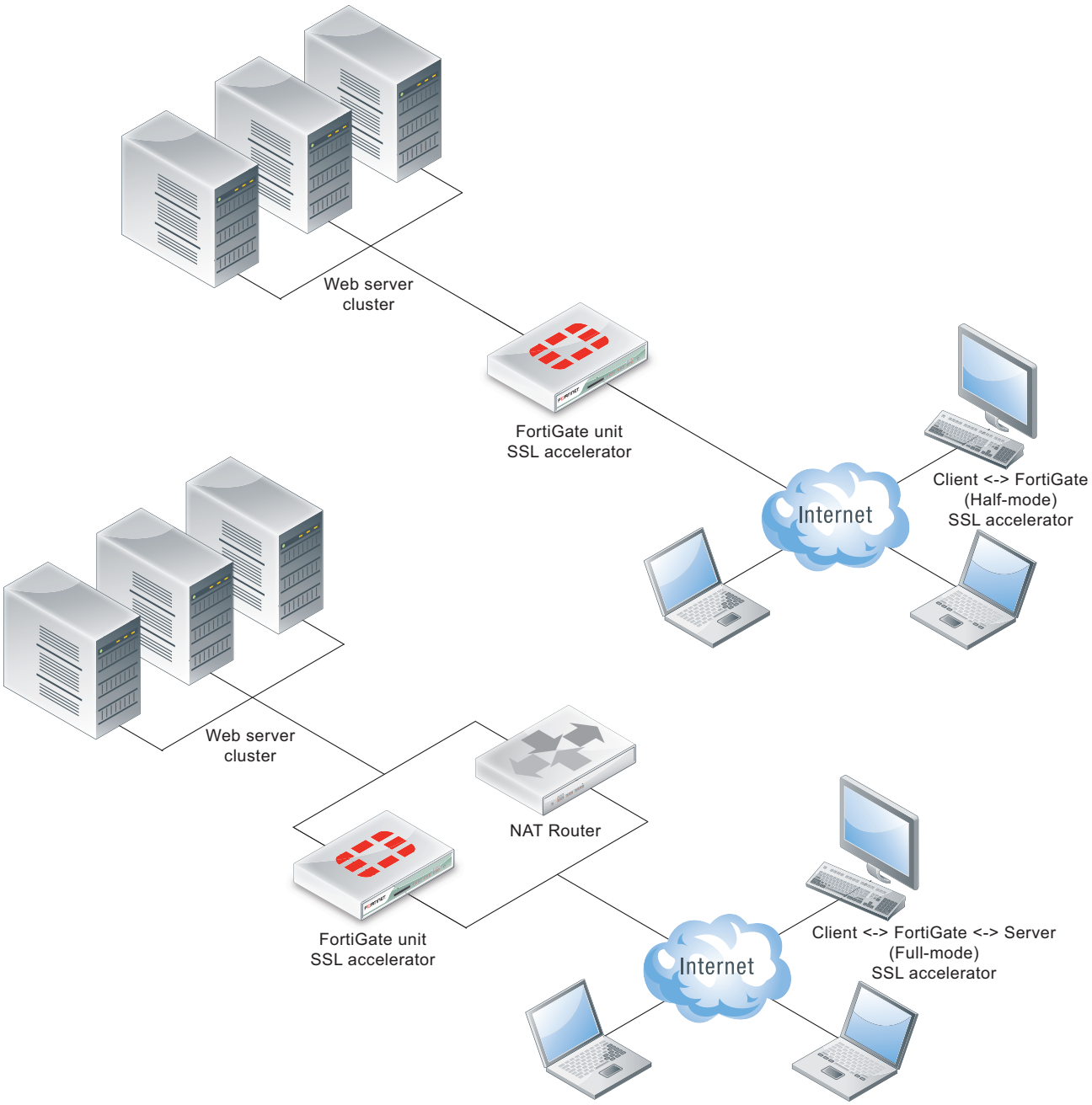
Use SSL offloading to accelerate clients' SSL or HTTPS connections to real servers by using the FortiGate unit to perform SSL operations (offloading them from the real servers using the FortiGate unit's SSL acceleration hardware). FortiGate units can offload SSL 3.0 and TLS 1.0. SSL offloading is available on FortiGate units that support SSL acceleration.

To configure SSL offloading from the web-based manager go to **Policy & Objects > Load Balance > Virtual Servers**. Add a virtual server and set the type to HTTPS or SSL and select the SSL offloading type (Client <-> FortiGate or Client <-> FortiGate <->Server).

Select Client <-> FortiGate to apply hardware accelerated SSL processing only to the part of the connection between the client and the FortiGate unit. This mode is called half mode SSL offloading. The segment between the FortiGate unit and the server will use clear text communications. This results in best performance, but cannot be used in failover configurations where the failover path does not have an SSL accelerator.

Select Client <-> FortiGate <->Server to apply hardware accelerated SSL processing to both parts of the connection: the segment between client and the FortiGate unit, and the segment between the FortiGate unit and the server. This mode is called full mode SSL offloading. The segment between the FortiGate unit and the server will use encrypted communications, but the handshakes will be abbreviated. This results in performance which is less than the other option, but still improved over communications without SSL acceleration, and can be used in failover configurations where the failover path does not have an SSL accelerator. If the server is already configured to use SSL, this also enables SSL acceleration without requiring changes to the server's configuration.

SSL Offloading modes



Configuring SSL offloading also requires selecting a certificate to use for the SSL offloading sessions. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

The following CLI command shows an example half mode HTTPS SSL offloading configuration. In the example the `ssl-mode` option sets the SSL offload mode to `half` (which is the default mode).

```
config firewall vip
   edit Vserver-ssl-offload
      set type server-load-balance
      set server-type https
```

```
        set ldb-method round-robin
        set extip 172.20.120.30
        set extintf wan1
        set extport 443
        set persistence ssl-session-id
        set ssl-mode half
        set ssl-certificate my-cert
        set monitor t cp-mon-1
           config realservers
              edit 1
                 set ip 10.31.101.30
                 set port 443
              next
              edit 2
                 set ip 10.31.101.40
                 set port 443
              end
     end
```

Additional SSL load balancing and SSL offloading options

The following SSL load balancing and SSL offloading options are only available from the CLI:

`ssl-client-session-state-max <sessionstates_int>`

Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit.

`ssl-client-session-state-timeout <timeout_int>`

Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the FortiGate unit.

`ssl-client-session-state-type {both | client | disable | time}`

Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate unit.

- `both`: Select to expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first.
- `count`: Select to expire SSL session states when `ssl-client-session-state-max` is exceeded.
- `disable`: Select to keep no SSL session states.
- `time`: Select to expire SSL session states when `ssl-client-session-state-timeout` is exceeded.

`ssl-dh-bits <bits_int>`

Enter the number of bits of the prime number used in the Diffie-Hellman exchange for RSA encryption of the SSL connection. Larger prime numbers are associated with greater cryptographic strength.

`ssl-http-location-conversion {enable | disable}`

Select to replace `http` with `https` in the reply's `Location` HTTP header field. For example, in the reply, `Location: http://example.com/` would be converted to `Location: https://example.com/`

`ssl-http-match-host {enable | disable}`

Select to apply `Location` conversion to the reply's HTTP header only if the host name portion of `Location` matches the request's `Host` field, or, if the `Host` field does not exist, the host name portion of the request's URI. If disabled, conversion occurs regardless of whether the host names in the request and the reply match.

For example, if host matching is enabled, and a request contains `Host: example.com` and the reply contains `Location: http://example.cc/`, the `Location` field does not match the host of the original request and

the reply's `Location` field remains unchanged. If the reply contains `Location: http://example.com/`, however, then the FortiGate unit detects the matching host name and converts the reply field to `Location: https://example.com/`.

This option appears only if `ssl-http-location-conversion` is `enable`.

`ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}`

Enter the maximum version of SSL/TLS to accept in negotiation. Support TLS 1.2 SSL offloading by specifying `tls-1.2`.

`ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}`

Enter the minimum version of SSL/TLS to accept in negotiation. Support TLS 1.2 SSL offloading by specifying `tls-1.2`.

`ssl-send-empty-frags {enable | disable}`

Select to precede the record with empty fragments to thwart attacks on CBC IV. You might disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.

`ssl-server-session-state-max <sessionstates_int>`

Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the server and the FortiGate unit.

`ssl-server-session-state-timeout <timeout_int>`

Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the server and the FortiGate unit. This option appears only if `ssl-mode` is `full`.

`ssl-server-session-state-type {both | count | disable | time}`

Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate unit. This option appears only if `ssl-mode` is `full`.

- `both`: Select to expire SSL session states when either `ssl-server-session-state-max` or `ssl-server-session-state-timeout` is exceeded, regardless of which occurs first.
- `count`: Select to expire SSL session states when `ssl-server-session-state-max` is exceeded.
- `disable`: Select to keep no SSL session states.
- `time`: Select to expire SSL session states when `ssl-server-session-state-timeout` is exceeded.

SSL offloading support for Internet Explorer 6

In some cases the Internet Explorer 6 web browser may be able to access real servers. To resolve this issue, disable the `ssl-send-empty-frags` option:

```
config firewall vip
   edit vip_name
      set ssl-send-empty-frags disable
   end
```

You can disable this option if SSL acceleration will be used with an old or buggy SSL implementation that cannot properly handle empty fragments.

Disabling SSL/TLS re-negotiation

The vulnerability CVE-2009-3555 affects all SSL/TLS servers that support re-negotiation. FortiOS when configured for SSL/TLS offloading is operating as a SSL/TLS server. The IETF is working on a TLS protocol change that will fix the problem identified by CVE-2009-3555 while still supporting re-negotiation. Until that protocol change is available, you can use the `ssl-client-renegotiation` option to disable support for

SSL/TLS re-negotiation. The default value of this option is `allow`, which allows an SSL client to renegotiate. You can change the setting to `deny` to abort any attempts by an SSL client to renegotiate. If you select `deny` as soon as a `ClientHello` message indicating a re-negotiation is received from the client FortiOS terminates the TCP connection.

Since SSL offloading does not support requesting client certificates the only circumstance in which a re-negotiation is required is when more than 2^32 bytes of data are exchanged over a single handshake. If you are sure that this volume of traffic will not occur then you can disable re-negotiation and avoid any possibility of the attack described in CVE-2009-3555.

The re-negotiation behavior can be tested using OpenSSL. The OpenSSL s_client application has the feature that the user can request that it do renegotiation by typing “R”. For example, the following shows a successful re-negotiation against a FortiGate unit configured with a VIP for 192.168.2.100:443:

```
$ openssl s_client -connect 192.168.2.100:443
   CONNECTED(00000003)
   depth=1 /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
   verify error:num=19:self signed certificate in certificate chain
   verify return:0
   ---
   Certificate chain
   0

    s:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Fortigate/CN=FW80CM3909604325/emailAdd
    ress=support@fortinet.com
      i:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
      Authority/CN=support/emailAddress=support@fortinet.com
   1 s:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
      i:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
      Authority/CN=support/emailAddress=support@fortinet.com
   ---
   Server certificate
-----BEGIN CERTIFICATE-----

---certificate not shown---

-----END CERTIFICATE-----

    subject=/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Fortigate/CN=FW80CM3909604325/em
    ailAddress=support@fortinet.com
   issuer=/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
   ---
   No client certificate CA names sent
   ---
   SSL handshake has read 2370 bytes and written 316 bytes
   ---
   New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
   Server public key is 1024 bit
   Compression: NONE
   Expansion: NONE
   SSL-Session:
      Protocol : TLSv1
      Cipher : DHE-RSA-AES256-SHA
      Session-ID:
      02781E1E368DCCE97A95396FAA82E8F740F5BBA96CF022F6FEC3597B0CC88095
```

```
    Session-ID-ctx:
    Master-Key:

   A6BBBD8477A2422D56E57C1792A4EA9C86F37D731E67D0A66E5CDB2B5C76650780C0E7F01CFF851EC44661
   86F4C48397
    Key-Arg : None
    Start Time: 1264453027
    Timeout : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate
    chain)
---
GET /main.c HTTP/1.0
R
RENEGOTIATING
depth=1 /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=support/emailAddress=support@fortinet.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
HTTP/1.0 200 ok
Content-type: text/plain

/*
* Copyright (C) 2004-2007 Fortinet
*/

#include <stdio.h>
#include "vsd_ui.h"

int main(int argc, char **argv)
{
return vsd_ui_main(argc, argv);
}
closed
$
```

The following is the same test, but this time with the VIP configuration changed to `ssl-client-renegotation deny`:

```
$ openssl s_client -connect 192.168.2.100:443
CONNECTED(00000003)
depth=1 /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=support/emailAddress=support@fortinet.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
0

 s:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Fortigate/CN=FW80CM3909604325/emailAdd
 ress=support@fortinet.com
   i:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
1 s:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=support/emailAddress=support@fortinet.com
   i:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
---
Server certificate
```

```
   -----BEGIN CERTIFICATE-----
---certificate not shown---
-----END CERTIFICATE-----

    subject=/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Fortigate/CN=FW80CM3909604325/em
    ailAddress=support@fortinet.com
   issuer=/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
   Authority/CN=support/emailAddress=support@fortinet.com
   ---
   No client certificate CA names sent
   ---
   SSL handshake has read 2370 bytes and written 316 bytes
   ---
   New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
   Server public key is 1024 bit
   Compression: NONE
   Expansion: NONE
   SSL-Session:
      Protocol : TLSv1
      Cipher : DHE-RSA-AES256-SHA
      Session-ID:
      8253331D266DDE38E4D8A04AFCA9CBDED5B1134932CE1718EED6469C1FBC7474
      Session-ID-ctx:
      Master-Key:

    ED05A3EF168AF2D06A486362FE91F1D6CAA55CEFC38A3C36FB8BD74236BF2657D4701B6C1456CEB5BB5EFA
    A7619EF12D
      Key-Arg : None
      Start Time: 1264452957
      Timeout : 300 (sec)
      Verify return code: 19 (self signed certificate in certificate
      chain)
   ---
   GET /main.c HTTP/1.0
   R
   RENEGOTIATING
19916:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:530:
```

Use the following command to check the SSL stats to see that the `renegotiations blocked` counter is now 1:

```
diagnose firewall vip virtual-server stats ssl
   ssl
      client
         connections total 0 active 0 max 0
         handshakes total 4 active 0 max 0 completed 4 abbreviated 0
         session states total 4 active 4 max 4
         cipher-suite failures 0
         embryonics total 0 active 0 max 0 terminated 0
         renegotiations blocked 1
      server
         connections total 0 active 0 max 0
         handshakes total 3 active 0 max 0 completed 2 abbreviated 1
         session states total 1 active 1 max 1
         cipher-suite failures 0
      internal error 0
      bad handshake length 0
      bad change cipher spec length 0
      pubkey too big 0
```

```
        persistence
          find 0 found 0 clash 0 addr 0 error 0
```

If the virtual server debug log is examined (diagnose debug appl vs -1) then at the point the re-negotiation is blocked there is a log:

```
vs ssl 12 handshake recv ClientHello
   vs ssl 12 handshake recv 1
       (0100005403014b5e056c7f573a563bebe0258c3254bbaff7046a461164f34f94f4f3d019c418000026
       003900380035001600130000a00330032002f0005000400150012000900140011000800060003020100
       00400230000)
   vs ssl 12 client renegotiation attempted rejected, abort
   vs ssl 12 closing 0 up
   vs src 12 close 0 in
   vs src 12 error closing
   vs dst 14 error closing
   vs dst 14 closed
   vs ssl 14 close
   vs sock 14 free
   vs src 12 closed
   vs ssl 12 close
   vs sock 12 free
```

IP, TCP, and UDP load balancing

You can load balance all IP, TCP or UDP sessions accepted by the security policy that includes a load balancing virtual server with the type set to IP, TCP, or UDP. Traffic with destination IP and port that matches the virtual server IP and port is load balanced. For these protocol-level load balancing virtual servers you can select a load balance method and add real servers and health checking. However, you can't configure persistence, HTTP multiplexing and SSL offloading.

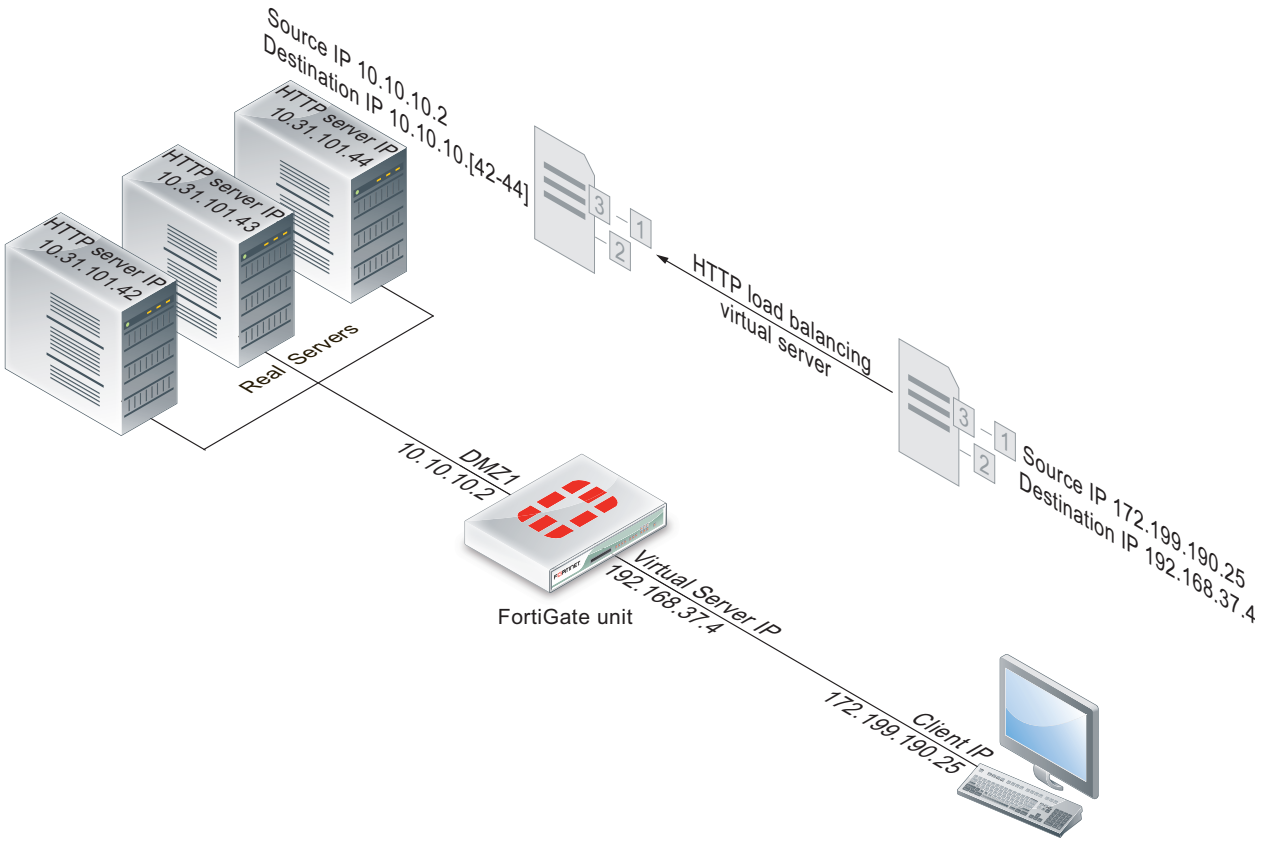
Load balancing configuration examples

Example HTTP load balancing to three real web servers

In this example, a virtual web server with IP address 192.168.37.4 on the Internet, is mapped to three real web servers connected to the FortiGate unit dmz1 interface. The real servers have IP addresses 10.10.123.42, 10.10.123.43, and 10.10.123.44. The virtual server uses the **First Alive** load balancing method. The configuration also includes an HTTP health check monitor that includes a URL used by the FortiGate unit for get requests to monitor the health of the real servers.

Connections to the virtual web server at IP address 192.168.37.4 from the Internet are translated and load balanced to the real servers by the FortiGate unit. First alive load balancing directs all sessions to the first real server. The computers on the Internet are unaware of this translation and load balancing and see a single virtual server at IP address 192.168.37.4 rather than the three real servers behind the FortiGate unit.

Virtual server configuration example



Web-based manager configuration

Use the following procedures to configure this load balancing setup from the web-based manager.

To add an HTTP health check monitor

In this example, the HTTP health check monitor includes the **URL** "/index.html" and the **Matched Phrase** "Fortinet products".

1. Go to **Policy & Objects > Load Balance > Health Check**.
2. Select **Create New**.
3. Add an HTTP health check monitor that sends get requests to http://<real_server_IP_address>/index.html and searches the returned web page for the phrase "Fortinet products".

Name	HTTP_health_chk_1
Type	HTTP
Port	80
URL	/index.html
Matched Content	Fortinet products
Interval	10 seconds
Timeout	2 seconds
Retry	3

4. Select **OK**.

To add the HTTP virtual server

1. Go to **Policy & Objects > Load Balance > Virtual Servers**.
2. Select **Create New**.
3. Add an HTTP virtual server that allows users on the Internet to connect to the real servers on the internal network. In this example, the FortiGate wan1 interface is connected to the Internet.

Name	Load_Bal_VS1
Type	HTTP
Interface	wan1

Virtual Server IP	192.168.37.4 The public IP address of the web server. The virtual server IP address is usually a static IP address obtained from your ISP for your web server. This address must be a unique IP address that is not used by another host and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP address.
Virtual Server Port	80
Load Balance Method	First Alive
Persistence	HTTP cookie
HTTP Multiplexing	Select. The FortiGate unit multiplexes multiple client into a few connections between the FortiGate unit and each real HTTP server. This can improve performance by reducing server overhead associated with establishing multiple connections.
Preserve Client IP	Select The FortiGate unit preserves the IP address of the client in the `X-Forwarded-For` HTTP header.
Health Check	Move the HTTP_health_chk_1 health check monitor to the **Selected** list.

4. Select **OK**.

To add the real servers and associate them with the virtual server

1. Go to **Policy & Objects > Load Balance > Real Servers**.
2. Select **Create New**.
3. Configure three real servers that include the virtual server Load_Bal_VS1. Each real server must include the IP address of a real server on the internal network.
   Configuration for the first real server.

Virtual Server	Load_Bal_VS1
IP Address	10.10.10.42
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.

Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

Configuration for the second real server.

Virtual Server	Load_Bal_VS1
IP Address	10.10.10.43
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

Configuration for the third real server.

Virtual Server	Load_Bal_VS1
IP Address	10.10.10.44
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

To add the virtual server to a security policy

Add a wan1 to dmz1 security policy that uses the virtual server so that when users on the Internet attempt to connect to the web server's IP address, packets pass through the FortiGate unit from the wan1 interface to the

dmz1 interface. The virtual IP translates the destination address of these packets from the virtual server IP address to the real server IP addresses.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Configure the security policy:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	wan1
Source Address	all (or a more specific address)
Outgoing Interface	dmz1
Destination Address	Load_Bal_VS1
Schedule	always
Service	HTTP
Action	ACCEPT
Log Allowed Traffic	Select to log virtual server traffic
Enable NAT	Select this option and select **Use Destination Interface Address**.

4. Select other security policy options as required.
5. Select **OK**.

CLI configuration

Use the following procedure to configure this load balancing setup from the CLI.

To configure HTTP load balancing

1. Use the following command to add an HTTP health check monitor that sends get requests to http://<real_server_IP_address>/index.html and searches the returned web page for the phrase “Fortinet products”.

```
config firewall ldb-monitor
   edit HTTP_health_chk_1
      set type http
      set port 80
      set http-get /index.html
      set http-match “Fortinet products”
      set interval 10
      set timeout 2
      set retry 3
   end
```

2. Use the following command to add an HTTP virtual server that allows users on the Internet to connect to the real servers on the internal network. In this example, the FortiGate wan1 interface is connected to the Internet.

```
config firewall vip
   edit Load-Bal_VS1
      set type server-load-balance
```

```
      set server-type http
      set ldb-method first-alive
      set http-multiplex enable
      set http-ip-header enable
      set extip 192.168.37.4
      set extintf wan1
      set extport 80
      set persistence http-cookie
      set monitor HTTP_health_chk_1
         config realservers
            edit 1
               set ip 10.10.10.42
               set port 80
            next
            edit 2
               set ip 10.10.10.43
               set port 80
            next
            edit 3
               set ip 10.10.10.44
               set port 80
         end
   end
```

3. Use the following command to add a security policy that includes the load balance virtual server as the destination address.

```
config firewall policy
   edit 0
      set srcintf wan1
      set srcaddr all
      set dstintf dmz1
      set dstaddr Load-Bal_VS1
      set action accept
      set schedule always
      set service ALL
      set nat enable
   end
```

Configure other security policy settings as required.

Example Basic IP load balancing configuration

This example shows how to add a server load balancing virtual IP that load balances all traffic among 3 real servers. In the example the Internet is connected to `port2` and the virtual IP address of the virtual server is 192.168.20.20. The load balancing method is `weighted`. The IP addresses of the real servers are 10.10.10.1, 10.10.10.2, and 10.10.10.3. The weights for the real servers are 1, 2, and 3. The default weight is 1 and does not have to be changed for the first real server.

```
config firewall vip
   edit All_Load_Balance
      set type server-load-balance
      set server-type ip
      set extintf port2
      set extip 192.168.20.20
      set ldb-method weighted
         config realservers
            edit 1
```

```
            set ip 10.10.10.1
        next
        edit 2
            set ip 10.10.10.2
            set weight 2
        next
        edit 3
            set ip 10.10.10.3
            set weight 3
        end
end
```

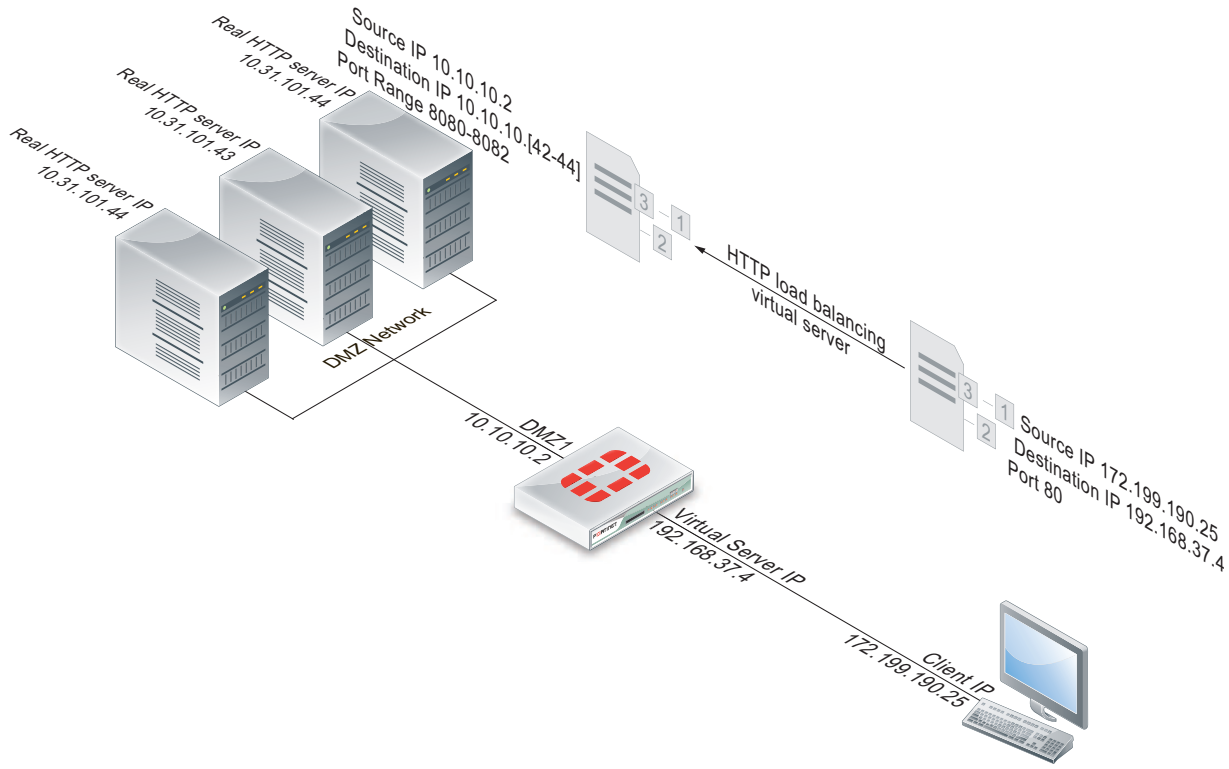
Example Adding a server load balance port forwarding virtual IP

In this example, a virtual web server with IP address 192.168.37.4 on the Internet, is mapped to three real web servers connected to the FortiGate unit dmz1 interface. The real servers have IP addresses 10.10.123.42, 10.10.123.43, and 10.10.123.44. The virtual server uses the **First Alive** load balancing method.

Each real server accepts HTTP connections on a different port number. The first real server accepts connections on port 8080, the second on port 8081, and the third on 8082. The configuration also includes an HTTP health check monitor that includes a URL used by the FortiGate unit for get requests to monitor the health of the real servers.

Connections to the virtual web server at IP address 192.168.37.4 from the Internet are translated and load balanced to the real servers by the FortiGate unit. First alive load balancing directs all sessions to the first real server. The computers on the Internet are unaware of this translation and load balancing and see a single virtual server at IP address 192.168.37.4 rather than the three real servers behind the FortiGate unit.

Server load balance virtual IP port forwarding



To complete this configuration, all of the steps would be the same as in Example HTTP load balancing to three real web servers on page 1880 except for configuring the real servers.

To add the real servers and associate them with the virtual server

Use the following steps to configure the FortiGate unit to port forward HTTP packets to the three real servers on ports 8080, 8081, and 8082.

1. Go to **Policy & Objects > Load Balance > Real Servers**.
2. Select **Create New**.
3. Configure three real servers that include the virtual server Load_Bal_VS1. Each real server must include the IP address of a real server on the internal network and have a different port number.

   Configuration for the first real server.

Virtual Server	Load_Bal_VS1
IP	10.10.10.42
Port	8080
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

   Configuration for the second real server.

Virtual Server	Load_Bal_VS1
IP	10.10.10.43
Port	8081
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

   Configuration for the third real server.

Virtual Server	Load_Bal_VS1
IP	10.10.10.44
Port	8082
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

Example Weighted load balancing configuration

This example shows how to using firewall load balancing to load balances all traffic among 3 real servers. In the example the Internet is connected to `port2` and the virtual IP address of the virtual server is 192.168.20.20. The load balancing method is `weighted`. The IP addresses of the real servers are 10.10.10.1, 10.10.10.2, and 10.10.10.3. The weights for the real servers are 1, 2, and 3.

This configuration does not include a health check monitor.

Web-based manager configuration

Use the following procedures to configure this load balancing setup from the web-based manager.

To add the HTTP virtual server

1. Go to **Policy & Objects > Load Balance > Virtual Servers**.
2. Select **Create New**.
3. Add an IP virtual server that allows users on the Internet to connect to the real servers on the internal network. In this example, the FortiGate port2 interface is connected to the Internet.

Name	HTTP_weghted_LB
Type	IP
Interface	port2
Virtual Server IP	192.168.20.20
Load Balance Method	Weighted

   All other virtual server settings are not required or cannot be changed.

4. Select **OK**.

To add the real servers and associate them with the virtual server

1. Go to **Policy & Objects > Load Balance > Real Servers**.
2. Select **Create New**.
3. Configure three real servers that include the virtual server All_Load _Balance. Because the **Load Balancing Method** is **Weighted**, each real server includes a weight. Servers with a greater weight receive a greater proportion of forwarded connections,

   Configuration for the first real server.

Virtual Server	HTTP_weghted_LB
IP Address	10.10.10.1
Port	Cannot be configured because the virtual server is an IP server.
Weight	1

Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

Configuration for the second real server.

Virtual Server	HTTP_weghted_LB
IP Address	10.10.10.2
Port	Cannot be configured because the virtual server is an IP server.
Weight	2
Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

Configuration for the third real server.

Virtual Server	HTTP_weghted_LB
IP Address	10.10.10.3
Port	Cannot be configured because the virtual server is an IP server.
Weight	3
Maximum Connections	0 Setting **Maximum Connections** to 0 means the FortiGate unit does not limit the number of connections to the real server. Since the virtual server uses **First Alive** load balancing you may want to limit the number of connections to each real server to limit the traffic received by each server. In this example, the **Maximum Connections** is initially set to 0 but can be adjusted later if the real servers are getting too much traffic.

To add the virtual server to a security policy

Add a port2 to port1 security policy that uses the virtual server so that when users on the Internet attempt to connect to the web server's IP address, packets pass through the FortiGate unit from the wan1 interface to the dmz1 interface. The virtual IP translates the destination address of these packets from the virtual server IP address to the real server IP addresses.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Configure the security policy:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	port2
Source Address	all (or a more specific address)
Outgoing Interface	port1
Destination Address	HTTP_weghted_LB
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Select this option and select **Use Destination Interface Address**.

4. Select other security policy options as required.
5. Select **OK**.

CLI configuration

Load balancing is configured from the CLI using the `config firewall vip` command and by setting `type` to `server-load-balance`. The default weight is 1 and does not have to be changed for the first real server.

Use the following command to add the virtual server and the three weighted real servers.

```
config firewall vip
   edit HTTP_weghted_LB
      set type server-load-balance
      set server-type ip
      set extintf port2
      set extip 192.168.20.20
      set ldb-method weighted
         config realservers
            edit 1
               set ip 10.10.10.1
            next
            edit 2
               set ip 10.10.10.2
               set weight 2
            next
            edit 3
               set ip 10.10.10.3
               set weight 3
            end
   end
```

Example HTTP and HTTPS persistence configuration

This example shows how to add a virtual server named **HTTP_Load_Balance** that load balances HTTP traffic using port 80 and a second virtual server named **HTTPS_Load_Balance** that load balances HTTPS traffic using port 443. The Internet is connected to port2 and the virtual IP address of the virtual server is 192.168.20.20. Both server load balancing virtual IPs load balance sessions to the same three real servers with IP addresses 10.10.10.2, 10.10.10.2, and 10.10.10.3. The real servers provide HTTP and HTTPS services.

For both virtual servers, persistence is set to **HTTP Cookie** to enable HTTP cookie persistence.

To add the HTTP and HTTPS virtual servers

1. Go to **Policy & Objects > Load Balance > Virtual Servers**.
2. Add the HTTP virtual server that includes HTTP Cookie persistence.

Name	HTTP_Load_Balance
Type	HTTP
Interface	port2
Virtual Server IP	192.168.20.20
Virtual Server Port	80 In this example the virtual server uses port 8080 for HTTP sessions instead of port 80.
Load Balance Method	Static
Persistence	HTTP cookie

3. Select **OK**.
4. Select **Create New**.
5. Add the HTTPs virtual server that also includes HTTP Cookie persistence.

Name	HTTPS_Load_Balance
Type	HTTPS
Interface	port2
Virtual Server IP	192.168.20.20
Virtual Server Port	443
Load Balance Method	Static
Persistence	HTTP cookie

6. Select **OK**.

To add the real servers and associate them with the virtual servers

1. Go to **Policy & Objects > Load Balance > Real Servers**.
2. Select **Create New**.
3. Configure three real servers for HTTP that include the virtual server HTTP_Load_Balance.

   Configuration for the first HTTP real server.

Virtual Server	HTTP_Load_Balance
IP Address	10.10.10.1
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

   Configuration for the second HTTP real server.

Virtual Server	HTTP_Load_Balance
IP Address	10.10.10.2
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

   Configuration for the third HTTP real server.

Virtual Server	HTTP_Load_Balance
IP Address	10.10.10.3
Port	80
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

4. Configure three real servers for HTTPS that include the virtual server HTTPS_Load_Balance.

   Configuration for the first HTTPS real server.

Virtual Server	HTTP_Load_Balance
IP Address	10.10.10.1

Port	443
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

Configuration for the second HTTPS real server.

Virtual Server	HTTP_Load_Balance
IP Address	10.10.10.2
Port	443
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

Configuration for the third HTTPS real server.

Virtual Server	HTTPS_Load_Balance
IP Address	10.10.10.3
Port	443
Weight	Cannot be configured because the virtual server does not include weighted load balancing.
Maximum Connections	0

To add the virtual servers to security policies

Add a port2 to port1 security policy that uses the virtual server so that when users on the Internet attempt to connect to the web server's IP address, packets pass through the FortiGate unit from the wan1 interface to the dmz1 interface. The virtual IP translates the destination address of these packets from the virtual server IP address to the real server IP addresses.

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Configure the HTTP security policy:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	port2
Source Address	all
Outgoing Interface	port1

Destination Address	HTTP_Load_Balance
Schedule	always
Service	HTTP
Action	ACCEPT
Enable NAT	Select this option and select **Use Destination Interface Address**.

4. Select other security policy options as required.
5. Select **OK**.
6. Select **Create New**.
7. Configure the HTTP security policy:

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	port2
Source Address	all
Outgoing Interface	port1
Destination Address	HTTPS_Load_Balance
Schedule	always
Service	HTTPS
Action	ACCEPT
Enable NAT	Select this option and select **Use Destination Interface Address**.

8. Select other security policy options as required.
9. Select **OK**.

CLI configuration: adding persistence for a specific domain

Load balancing is configured from the CLI using the `config firewall vip` command and by setting `type` to `server-load-balance`.

For the CLI configuration, both virtual servers include setting `http-cookie-domain` to `.example.org` because HTTP cookie persistence is just required for the `example.org` domain.

First, the configuration for the HTTP virtual IP:

```
config firewall vip
   edit HTTP_Load_Balance
      set type server-load-balance
      set server-type http
      set extport 8080
      set extintf port2
      set extip 192.168.20.20
      set persistence http-cookie
```

```
      set http-cookie-domain .example.org
         config realservers
            edit 1
               set ip 10.10.10.1
            next
            edit 2
               set ip 10.10.10.2
            next
            edit 3
               set ip 10.10.10.3
            end
   end
```

Second, the configuration for the HTTPS virtual IP. In this configuration you don't have to set `extport` to `443` because `extport` is automatically set to `443` when `server-type` is set to `https`.

```
config firewall vip
   edit HTTPS_Load_Balance
      set type server-load-balance
      set server-type https
      set extport 443
      set extintf port2
      set extip 192.168.20.20
      set persistence http-cookie
      set http-cookie-domain .example.org
         config realservers
            edit 1
               set ip 10.10.10.1
            next
            edit 2
               set ip 10.10.10.2
            next
            edit 3
               set ip 10.10.10.3
            end
   end
```

Chapter 18 - Logging and Reporting

This FortiOS Handbook chapter contains the following sections:

Logging and reporting overview provides general information about logging. We recommend that you begin with this chapter as it contains information for both beginners and advanced users as well. It contains an explanation of log messages, files, and devices, and an overview of the Reporting functions.

Logging and reporting for small networks provides an overview of setting up a small network for logging, with a look at a possible setup with a backup solution and a customized report.

Logging and reporting for large networks provides an overview of setting up a larger, enterprise-level network, with configuration of multiple FortiGate units, multiple FortiAnalyzer units as a backup solution, and a sample procedure for creating a more intensive and broad report to suit the larger network.

Advanced logging provides a series of separate tutorials for possible tasks and procedures an advanced user may want to undertake with their FortiGate-powered network. It contains explanations of advanced backup, logging, and report solutions.

Troubleshooting and logging provides a short overview of how log messages can be used to identify and solve problems within the network, how to identify and solve logging database issues, and how to solve connection issues between FortiGate and FortiAnalyzer units.

Logging and reporting overview

Logging and reporting in FortiOS can help you in determining what is happening on your network, as well as informing you of certain network activity, such as detection ofa virus or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information as well as helping to show others the activity that is happening on the network.

This section explains logging and reporting features that are available in FortiOS, and how they can be used to help you manage or troubleshoot issues. This includes how the FortiGate unit records logs, what a log message is, and what the log database is.

What is logging?

Logging records the traffic passing through the FortiGate unit to your network and what action the FortiGate unit took during its scanning process of the traffic. This recorded information is called a log message.

After a log message is recorded, it is stored within a log file which is then stored on a log device. A log device is a central storage location for log messages. The FortiGate unit supports several log devices, such as FortiAnalyzer units, the FortiCloud service, and Syslog servers. A FortiGate unit's system memory and local disk can also be configured to store logs, and because of this, are also considered log devices.

You must subscribe to FortiCloud before you will be able to configure the FortiGate unit to send logs to a FortiCloud server.

When the recorded activity needs to be read in a more human way, the FortiGate unit can generate a Report. A report gathers all the log information that is needed for the report, and presents it in a graphical format, with customizable design and automatically generated charts. Reports can be used to present a graphical representation of what is going on in the network. Reports can also be generated on a FortiAnalyzer unit; if you want to generate reports on a FortiAnalyzer, see the FortiAnalyzer Setup and Administration Guide to help you create and generate those reports.

How the FortiGate unit records log messages

The FortiGate unit records log messages in a specific order, storing them on a log device. The order of how the FortiGate unit records log messages is as follows:

1. Incoming traffic is scanned.
2. During the scanning process, the FortiGate unit performs necessary actions, and simultaneously records the actions and results.
3. Log messages are sent to the log device.

Example: How the FortiGate unit records a DLP event

1. The FortiGate unit receives incoming traffic and scans for any matches associated within its firewall policies containing a DLP sensor.

2. A match is found; the DLP sensor, dlp_sensor, had a rule within it called All-HTTP with the action Exempt applied to the rule. The sensor also has Enable Logging selected, which indicates to the FortiGate unit that the activity should be recorded and placed in the DLP log file.
3. The FortiGate unit exempts the match, and places the recorded activity (the log message) within the DLP log file.
4. According to the log settings that were configured, logs are stored on the FortiGate unit's local hard drive. The FortiGate unit places the DLP log file on the local hard drive.

FortiOS features available for logging

Logs record FortiGate activity, providing detailed information about what is happening on your network. This recorded activity is found in log files, which are stored on a log device. However, logging FortiGate activity requires configuring certain settings so that the FortiGate unit can record the activity. These settings are often referred to as log settings, and are found in most security profiles, but also in **Log & Report > Log Config > Log Settings**.

Log settings provide the information that the FortiGate unit needs so that it knows what activities to record. This topic explains what activity each log file records, as well as additional information about the log file, which will help you determine what FortiGate activity the FortiGate unit should record.

Traffic

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

Logging traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic)
- packet comes into an inbound interface
- a possible log packet is sent regarding a match in the firewall policy, such as a URL filter
- traffic log packet is sent, per firewall policy
- packet passes and is sent out an interface

Traffic log messages are stored in the traffic log file. Traffic logs can be stored any log device, even system memory.

All security profile-related logs are now tracked within the Traffic logs, as of FortiOS 5.0, so all forward traffic can be searched in one place, such as if you are looking to see all activity from a particular address, security feature or traffic. Security profile logs are still tracked separately in the **Security Log** section, which only appears when logs exist.

If you have enabled and configured WAN Optimization, you can enable logging of this activity in the CLI using the `config wanopt setting` command. These logs contain information about WAN Optimization activity and are found in the traffic log file. When configuring logging of this activity, you must also enable logging within the security policy itself, so that the activity is properly recorded.

Sniffer

The Sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the Traffic logs.

Other Traffic

The traffic log also records interface traffic logging, which is referred to as Other Traffic. Other Traffic is enabled only in the CLI. When enabled, the FortiGate unit records traffic activity on interfaces as well as firewall policies. Logging Other Traffic puts a significant system load on the FortiGate unit and should be used only when necessary.

Logging other traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic) and other-traffic
- packet comes into an interface
- interface log packet is sent to the traffic log that is enabled on that particular interface
- possible log packet is sent regarding a match in the firewall policy, such as URL filter
- interface log packet is sent to the traffic log if enabled on that particular interface
- packet passes and is sent out an interface
- interface log packet is sent to traffic (if enabled) on that particular interface

Event

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Event logs help you in the following ways:

- keeping track of configuration setting changes
- IPsec negotiation, SSL VPN and tunnel activity
- quarantine events, such as banned users
- system performance
- HA events and alerts
- firewall authentication events
- wireless events on models with WiFi capabilities
- activities concerning modem and internet protocols L2TP, PPP and PPPoE
- VIP activities
- AMC disk's bypass mode
- VoIP activities that include SIP and SCCP protocols.

The FortiGate unit records event logs only when events are enabled.

Traffic Shaping

Traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings can be applied to a firewall policy, appearing within the traffic log messages.

By enabling this feature, you can see what traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings are being used.

Data Leak Prevention

Data Leak Prevention logs, or DLP logs, provide valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP rules within a DLP sensor can log the following traffic types:

- email (SMTP, POP3 or IMAP; if SSL content SMTPS, POP3S, and IMAPS)
- HTTP
- HTTPS
- FTP
- NNTP
- IM

A DLP sensor must have log settings enabled for each DLP rule and compound rule, as well as applied to a firewall policy so that the FortiGate unit records this type of activity. A DLP sensor can also contain archiving options, which these logs are then archived to the log device.

NAC Quarantine

Within the DLP sensor, there is an option for enabling NAC Quarantine. The NAC Quarantine option allows the FortiGate unit to record details of DLP operation that involve the ban and quarantine actions, and sends these to the event log file. The NAC Quarantine option must also be enabled within the Event Log settings. When enabling NAC quarantine within a DLP Sensor, you must enable this in the CLI because it is a CLI-only command.

Media Access Control (MAC) Address

MAC address logs provide information about MAC addresses that the FortiGate unit sees on the network as well as those removed from the network. These log messages are stored in the event log (as subtype network; you can view these log messages in **Log & Report > Event Log**) and are, by default, disabled in the CLI. You can enable logging MAC addresses using the following command syntax:

```
config log setting
   set neighbor-event enable
end
```

When enabled, a new log message is recorded every time a MAC address entry is added to the ARP table, and also when a MAC address is removed as well. A MAC address log message is also recorded when MAC addresses are connected to the local switch, or from a FortiAP or FortiSwitch unit.

Application control

Application control logs provide detailed information about the traffic that internet applications such as Skype are generating. The application control feature controls the flow of traffic from a specific application, and the FortiGate unit examines this traffic for signatures that the application generates.

The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiGate unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called application control monitoring and you can view the information from a widget on the Executive Summary page.

The application control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for application control records the packet when an application type is identified, similar to IPS packet logging.

Logging of application control activity can only be recorded when an application control list is applied to a firewall policy, regardless of whether or not logging is enabled within the application control list.

Antivirus

Antivirus logs are recorded when, during the antivirus scanning process, the FortiGate unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature. Antivirus logs provide a way to understand what viruses are trying to get in, as well as additional information about the virus itself, without having to go to the FortiGuard Center and do a search for the detected virus. The link is provided within the log message itself.

These logs provide valuable information such as:

- the name of the detected virus
- the name of the oversized file or infected file
- the action the FortiGate unit took, for example, a file was blocked
- URL link to the FortiGuard Center which gives detailed information about the virus itself

The antivirus profile must have log settings enabled within it so that the FortiGate unit can record this activity, as well as having the antivirus profile applied to a firewall policy.

Web Filter

Web filter logs record HTTP traffic activity. These log messages provide valuable and detailed information about this particular traffic activity on your network. Web filtering activity is important to log because it can inform you about:

- what types of web sites employees are accessing
- users attempting to access banned web sites and how often this occurs
- network congestion due to employees accessing the Internet at the same time
- web-based threats resulting from users visiting non-business-related web sites

Web Filter logs are an effective tool to help you determine if you need to update your web filtering settings within a web filter profile due to unforeseen threats or network congestion. These logs also inform you about web filtering quotas that have been configured for filtering HTTP traffic.

You must configure logging settings within the web filter profile and apply the filter to a firewall policy so that the FortiGate unit can record the activity.

IPS (attack)

IPS logs, also referred to as attack logs, record attacks that occurred against your network. Attack logs contain detailed information about whether the FortiGate unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was.

The IPS or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiGate unit.

An IPS sensor with log settings enabled must be applied to a firewall policy so that the FortiGate unit can record the activity.

Packet logs

When you enable packet logging within an IPS signature override or filter, the FortiGate unit examines network packets, and if a match is found, saves them to the attack log. Packet logging is designed to be used as a diagnostic tool that can focus on a narrow scope of diagnostics, rather than a log that informs you of what is occurring on your network.

You should use caution when enabling packet logging, especially within IPS filters. Filter configuration that contains thousands of signatures could potentially cause a flood of saved packets, which would take up a lot of storage space on the log device. It would also take a great deal of time to sort through all the log messages, as well as consume considerable system resources to process.

You can archive packets, but you must enable this option on the Log Settings page. If your log configuration includes multiple FortiAnalyzer units, packet logs are only sent to the primary (first) FortiAnalyzer unit. Sending packet logs to the other FortiAnalyzer units is not supported.

Email filter

Email filter logs, also referred to as spam filter logs, records information regarding the content within email messages. For example, within an email filter profile, a match is found that finds the email message to be considered spam.

Email filter logs are recorded when the FortiGate unit finds a match within the email filter profile and logging settings are enabled within the profile.

Archives (DLP)

Recording DLP logs for network use is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Archived logs are usually saved for historical use and can be accessed at any time. IPS packet logs can also be archived, within the Log Settings page.

You can start with the two default DLP sensors that have been configured specifically for archiving log data, Content_Archive and Content_Summary. They are available in **Security Profiles > Data Leak Prevention**. Content_Archive provides full content archiving, while Content_Summary provides summary archiving. For more information about how to configure DLP sensors, see the Security Features chapter of the FortiOS Handbook.

You must enable the archiving to record log archives. Logs are not archived unless enabled, regardless of whether or not the DLP sensor for archiving is applied to the firewall policy.

Network scan

Network scan logs are recorded when a scheduled scan of the network occurs. These log messages provide detailed information about the network's vulnerabilities regarding software, as well as the discovery of any further vulnerabilities.

A scheduled scan must be configured and logging enabled within the Event Log settings, for the FortiGate unit to record these log messages.

Log messages

Log messages are recorded by the FortiGate unit, giving you detailed information about the network activity. Each log message has a unique number that helps identify it, as well as containing fields; these fields, often called log fields, organize the information so that it can be easily extracted for reports.

These log fields are organized in such a way that they form two groups: the first group, made up of the log fields that come first, is called the log header. The log header contains general information, such as the unique log identification and date and time that indicates when the activity was recorded. The log body is the second group, and contains all the other information about the activity. There are no two log message bodies that are alike, however, there may be fields common to most log bodies, such as the `srcintf` or `identidix` log fields.

The log header also contains information about the log priority level which is indicated in the `level` field. The priority level indicates the immediacy and the possible repercussions of the logged action. For example, if the field contains 'alert', you need to take immediate action with regards to what occurred. There are six log priority levels.

The log severity level is the level at and above which the FortiGate unit records logs. The log severity level is defined by you when configuring the logging location. The FortiGate unit will log all messages at and above the priority level you select. For example, if you select Error, the unit will log only Error, Critical, Alert, and Emergency level messages.

Log priority levels

Levels	Description
0 - Emergency	The system has become unstable.
1 - Alert	Immediate action is required.
2 - Critical	Functionality is affected.
3 - Error	An error condition exists and functionality could be affected.
4 - Warning	Functionality could be affected.
5 - Notification	Information about normal events.
6 - Information	General information about system operations.

The Debug priority level, not shown above, is rarely used. It is the lowest log priority level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly.

Example log header fields

Log header	
date=(2010-08-03)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:55:06)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
log_id=(2457752353)	A five or ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message.
type=(dlp)	The section of system where the event occurred.
subtype=(dlp)	The subtype category of the log message.
level=(notice)	The priority level of the event. See the table above.
vd=(root)	The name of the virtual domain where the action/event occurred in. If no virtual domains exist, this field always contains root.

Example log body fields

Log body	
policyid=(1)	The ID number of the firewall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero.
identidx=(0)	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid=(311)	The serial number of the firewall session of which the event happened.
srcip=(10.10.10.1)	The source IP address.
srcport=(1190)	The source port number.
srcintf=(internal)	The source interface name.
dstip=(192.168.1.122)	The destination IP address.
dstport=(80)	The destination port number.
dstintf=(wan1)	The destination interface name.
service=(https)	The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policy.
status=(detected)	The action the FortiGate unit took.
hostname=(example.com)	The home page of the web site.
url=(/image/trees_pine_ forest/)	The URL address of the web page that the user was viewing.
msg=(data leak detected (Data Leak Prevention Rule matched)	Explains the FortiGate activity that was recorded. In this example, the data leak that was detected matched the rule, All-HTTP, in the DLP sensor.
rulename=(All-HTTP)	The name of the DLP rule within the DLP sensor.
action=(log-only)	The action that was specified within the rule. In some rules within sensors, you can specify content archiving. If no action type is specified, this field display log-only.
severity=(1)	The level of severity for that specific rule.

Logs from other devices, such as the FortiAnalyzer unit and Syslog server, contain a slightly different log header. For example, when viewing FortiGate log messages on the FortiAnalyzer unit, the log header contains the following log fields when viewed in the Raw format:

```
itime=1302788921 date=20110401 time=09:04:23 devname=FG50BH3G09601792 device_
    id=FG50BH3G09601792 log_id=0100022901 type=event subtype=system level=notice vd=root
```

The log body contains the rest of the information of the log message, and this information is unique to the log message itself.

For detailed information on all log messages, see the *FortiGate Log Message Reference*.

Explanation of a debug log message

Debug log messages are only generated if the log severity level is set to Debug. The Debug severity level is the lowest log severity level and is rarely used. This severity level usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are generated by all types of FortiGate features.

The following is an example of a debug log message:

```
date=2010-01-25 time=17:25:54 logid=9300000000 type=webfilter subtype=urlfilter
    level=debug msg="found in cache"
```

Example of a Debug log message

Debug log	
date=(2010-01-25)	The year, month and day of when the event occurred in the format yyyy-mm-dd.
time=(17:25:54)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
logid=(93000000000)	A ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message.
type=(webfilter)	The section of system where the event occurred. There are eleven log types in FortiOS 5.2.
subtype=(urlfilter)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
level=(debug)	The priority level of the event. There are six priority levels to specify.
msg=("found in cache")	Explains the activity or event that the FortiGate unit recorded.

Viewing log messages and archives

Depending on the log device, you may be able to view logs within the web-based manager or CLI on the FortiGate unit. If you have configured a FortiAnalyzer unit, local hard disk, or system memory, you can view log messages from within the web-based manager or CLI. If you have configured either a Syslog or WebTrends server, you will not be able to view log messages from the web-based manager or CLI. There is also no support for viewing log messages stored on a FortiCloud server, from the FortiGate unit's web-based manager or CLI.

You do not have to view log messages from only the web-based manager. You can view log messages from the CLI as well, using the `execute log display` command. This command allows you to see specific log messages that you already configured within the `execute log filter` command. The `execute log filter` command configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view. For more information about viewing log messages in the CLI, see "Viewing logs from the CLI".

There are two log viewing options in FortiOS: Format and Raw. The Raw format displays logs as they appear within the log file. You can view log messages in the Raw format using the CLI or a text editor, such as Notepad. Format is in a more human-readable format, and you can easily filter information when viewing log messages this way. The Format view is what you see when viewing logs in the web-based manager.

When you download the log messages from within the log message page (for example, **Log & Report > Traffic Log > Forward Traffic**), you are downloading log messages in the Raw format.

Viewing log messages in detail

From any log page, you can view detailed information about the log message in the log viewer table, located (by default) at the bottom of the page. Each page contains this log viewer table. The Log Viewer Table can contain the Archive tab, which allows you to see the archived version of the log message. The Archive tab only displays the archived log's details if archiving is enabled and logs are being archived by the FortiGate unit, but archived logs will also be recorded when using a FortiAnalyzer unit or the FortiCloud service.

When you are viewing traffic log messages, some of the categories (such as 'Application Name') have entries that can be selected to open a dialog box containing FortiGuard information about the entry. From within the dialog box, you can select the Reference link and go directly to the corresponding FortiGuard page, which contains additional information.

Viewing logs in Raw format allows you to view all log fields at once, as well as have a log file available regardless of whether you are archiving logs or not. You download the log file by selecting **Download Raw Log**. The log file is named in the following format: <log_type><log_location><log_date/time>.<log_number>.log. For example, SystemEventLog-disk-2012-09-19T12_13_46.933949.log, which is an event log. The time period is the day and month of when the log was downloaded, not the time period of the log messages within the file itself.

Quarantine

Within the Log & Report menu, you can view detailed information about each quarantined file. The information can either be sorted or filtered, depending on what you want to view.

You must enable quarantine settings within an antivirus profile and the destination must be configured in the CLI using the `config antivirus quarantine` command. The destination can be either a FortiAnalyzer unit or local disk.

Sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). Filter the list to view only quarantined files with a specific status or from a specific service.

On **Log & Report > Security Log > Quarantine**, the file quarantine list displays the following information about each quarantined file.

Quarantine page

Lists all files that are considered quarantined by the unit. On this page you can filter information so that only specific files are displayed on the page.

GUI Item	Description
Source	Either **FortiAnalyzer** or **Local Disk**, depending where you configure to quarantined files to be stored.
Sort by	Sort the list. Choose from: **Status**, **Service**, **File Name**, **Date**, **TTL**, or **Duplicate Count**. Select **Apply** to complete the sort.
Filter	Filter the list. Choose either **Status** (infected, blocked, or heuristics) or **Service** (IMAP, POP3, SMTP, FTP, HTTP, MM1, MM3, MM4, MM7, IM, or NNTP). Select **Apply** to complete the filtering. Heuristics mode is configurable through the CLI only. If your unit supports SSL content scanning and inspection Service can also be IMAPS, POP3S, SMTPS, or HTTPS. For more information, see the Security Features chapter of the FortiOS Handbook.
Apply	Select to apply the sorting and filtering selections to the list of quarantined files.
Delete	Select to delete the selected files.
Page Controls	Use the controls to page through the list.
Remove All Entries	Removes all quarantined files from the local hard disk. This icon only appears when the files are quarantined to the hard disk.
File Name	The file name of the quarantined file. When a file is quarantined, all spaces are removed from the file name, and a 32-bit checksum is performed on the file. The checksum appears in the replacement message but not in the quarantined file. The file is stored on the FortiGate hard disk with the following naming convention: <32bit_CRC>.<processed_filename> For example, a file named Over Size.exe is stored as 3fc155d2.oversize.exe.
Date	The date and time the file was quarantined, in the format dd/mm/yyyy hh:mm. This value indicates the time that the first file was quarantined if duplicates are quarantined.
Service	The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP, MM1, MM3, MM4, MM7, IM, NNTP, IMAPS, POP3S, SMTPS, or HTTPS).
Status	The reason the file was quarantined: **infected**, **heuristics**, or **blocked**.
Status Description	Specific information related to the status, for example, “File is infected with “W32/Klez.h”” or “File was stopped by file block pattern.”

GUI Item	Description
DC	Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak.
TTL	Time to live in the format hh:mm. When the TTL elapses, the FortiGate unit labels the file as EXP under the TTL heading. In the case of duplicate files, each duplicate found refreshes the TTL. The TTL information is not available if the files are quarantined on a FortiAnalyzer unit.
Upload status	**Y** indicates the file has been uploaded to Fortinet for analysis, **N** indicates the file has not been uploaded. This option is available only if the FortiGate unit has a local hard disk.
Download	Select to download the corresponding file in its original format. This option is available only if the FortiGate unit has a local hard disk.
Submit	Select to upload a suspicious file to Fortinet for analysis. This option is available only if the FortiGate unit has a local hard disk.

Customizing the display of log messages on the web-based manager

Customizing log messages on the web-based manager allows you to remove or add columns from the page and filter the information that appears. For example, you can view only log messages that appeared on December 4, between the hours of 8:00 and 8:30 am.

1. Select the submenu in **Log & Report** in which you want to customize the display of log messages, such as **Log & Report > Traffic Log > Forward Traffic**.
2. Right click on the title bar at the top of any column, and uncheck a column title such as **Date/Time** to remove it from the interface. Check other columns to add them to the interface. When you are finished, click outside the menu and the page will refresh with the new column settings in place.
3. Choose a column you'd like to filter, and select the funnel icon next to the title of the column. For example, select the funnel in the Src (Source) column. In the text field, enter the source IP address 1.1.1.1 and then select the check box beside **NOT**.
   This filters out the all log messages that have the 1.1.1.1 source IP address in the source IP log field, such as the ones generated when running log tests in the CLI.
4. Select **OK** to save the customize settings, and then view the log messages on the page.
   Log messages that originate from the 1.1.1.1 source address will no longer appear in the list.

How to download log messages and view them from on a computer

After recording some activity, you can download log messages to view them from a computer. This is can be very useful when in a remote location, or if you want to view log messages at your convenience, or to view packet logs or traffic logs.

1. In Log & Report, select the submenu that you want to download log messages from.
   For example, **Log & Report > Traffic Log> Forward Traffic**.

2. Select the **Download Raw Log** option and save the log file to your computer.
   The log file will be downloaded like any other file. Log file names contain their log type and date in the name, so it is recommended to create a folder in which to archive your log messages, as they can be sorted easily.
3. Open a text editor such as Notepad, open the log file, and then scroll to view all the log messages.
   You can easily search or scroll through the logs to see the information that is available.

Log files and types

As the log messages are being recorded, log messages are also being put into different log files. The log file contains the log messages that belong to that log type, for example, traffic log messages are put in the traffic log file.

When downloading the log file from within **Log & Report**, the file name indicates the log type and the device on which it is stored, as well as the date, time, and a unique id for that log.

This name is in the format <logtype> - <logdevice> - <date> T <time> . <id>.log.

For example, AntiVirusLog-disk-2012-09-13T11_07_57.922495.log.

Below, each of the different log files are explained. Traffic and Event logs come in multiple types, but all contain the base type such as ‘Event’ in the filename.

Log Types based on network traffic

Log Type	Description
Traffic	The traffic logs records all traffic to and through the FortiGate interface. Different categories monitor different kinds of traffic, whether it be forward, local, or sniffer.
Event	The event logs record management and activity events within the device in particular areas: System, Router, VPN, User, Endpoint, HA, WAN Opt./Cache, and WiFi. For example, when an administrator logs in or logs out of the web-based manager, it is logged both in System and in User events.
Antivirus	The antivirus log records virus incidents in Web, FTP, and email traffic.
Web Filter	The web filter log records HTTP FortiGate log rating errors including web content blocking actions that the FortiGate unit performs.
Application Control	The application log records application usage, monitoring or blocking as configured in the security profiles.
Intrusion	The intrusion log records attacks that are detected and prevented by the FortiGate unit.
Email Filter	The email filter log records blocking of email address patterns and content in SMTP, IMAP, and POP3 traffic.
Vulnerability Scan	The Vulnerability Scan (Netscan) log records vulnerabilities found during the scanning of the network.
Data Leak Prevention	The Data Leak Prevention log records log data that is considered sensitive and that should not be made public. This log also records data that a company does not want entering their network.
VoIP	The VoIP log records VoIP traffic and messages. It only appears if VoIP is enabled on the Administrator Settings page.

Log database and datasets

The log database, also known as the SQL log database, is used to store logs on FortiGate units that have a built-in hard disk. The log database uses Structured Query Lanaguage (SQL), specifically it uses SQLite which is an embedded Relational Database Management System (RDBMS).

If you have disabled SQL logging and have factory defaults on the FortiGate unit, and then you upgrade the firmware, the upgrade will automatically disable SQL logging. When this occurs, you must re-enable SQL logging manually.

The FortiGate unit creates a database table for each log type, when log data is recorded. If the FortiGate unit is not recording log data, it does not create log tables for that device.

The command syntax, `get report database schema`, allows you to view all the tables, column names and types that are available to use when creating SQL statements for datasets.

If you want to view the size of the database, as well as the log database table entries, use the `get log sql status` command. This command displays the amount of free space that is available as well as the first and last log database entry time and date.

The output of the `get log sql status` command contains information similar to the following:

```
Database size: 294912
Free size in database: 0
Database Page Size: 8192
Entry number:
Event: 49
Traffic: 370
Attack: 2
AntiVirus: 4
WebFilter: 254
AntiSpam: 2
Netscan: 18
Total: 699
First entry time: 2012-09-10 11:41:02
Last entry time: 2012-09-13 02:59:59
```

The log database is not only used to store logs, but also used to extract the information for reports. Reports are built from datasets, which are SQL statements that tell the FortiGate unit how to extract the information from the database. You can create your own datasets; however, SQL knowledge is required. Default datasets are available for reports.

Notifications about network activity

Alert email messages provide notification about activities or events logged. These email messages also provide notification about log severities that are recorded, such as a critical or emergency.

You can send alert email messages to up to three email addresses. Alert messages are also logged and can be viewed from the Event Log menu, in the System Event log file.

You can use the alert email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out. You can also base alert email messages on the severity levels of the logs. The FortiGate unit does not currently support SSL/TLS connections for SMTP servers, so you must choose an SMTP server that does not need SSL/TLS when configuring the SMTP server settings.

Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

The default minimum log severity level is Alert. If the FortiGate unit collects more than one log message before an interval is reached, the FortiGate unit combines the messages and sends out one alert email.

How to configure email notifications

The following explains how to configure an alert email notification for IPsec tunnel errors, firewall authentication failure, configuration changes and FortiGuard license expiry.

1. In **System > Config > Advanced**, under **Email Service**, configure the SMTP server.
   The SMTP server settings allow the FortiGate unit to know exactly where the email will be sent from, as well as who to send it to. The SMTP server must be a server that does not support SSL/TLS connections; if the SMTP server does, the alert email configuration will not work. The FortiGate unit does not currently support SSL/TLS connections for SMTP servers.
2. In **Log & Report > Log Config > Alert E-mail**, enter the source email in the Email From field, and up to three target addresses in the Email To fields.
3. Below the email entry, you can configure the email responses. By default, the **Send alert email for the following** is enabled. Select the check boxes beside **IPsec tunnel errors**, **Configuration changes** and **Firewall authentication failure**.
   These alerts will be sent to the email address specified when the trigger occurs. For example, a user attempts to connect to the branch office of the company but cannot; the FortiGate unit detects an IPsec tunnel error, records the event, and then sends the notice to the email address specified in the SMTP server settings.
4. Select **FortiGuard license expiry time:** and then enter 10 so that the email notification will be sent ten days prior to the FortiGuard license expiration.
   You can choose up to 100 days prior to when the license will expire. The default time is 15 days. By using this alert email notification, you can easily know when to send an re-registration request long before the expiry.

Log devices

The FortiGate unit supports a variety of log devices, including the FortiCloud service and FortiAnalyzer units. This provides greater flexibility not only when choosing a log device, but also when your logging requirements need updating.

When you have developed a plan that meets your logging needs and requirements, you need to select the log device that is appropriate for that plan. A log device must be able to store all the logs you need, and if you require archiving those logs, you must consider what log devices support this option.

During this process of deciding what log device meets your needs and requirements, you must also figure out how to provide a backup solution in the event the log device that the FortiGate unit is sending logs to has become unavailable. A backup solution should be an important part of your log setup because it helps you to maintain all logs and prevents lost logs, or logs that are not sent to the log device. For example, a daily backup of log files to the FortiAnalyzer unit occurs at 5 pm.

Log devices provide a central location for storing logs recorded by the FortiGate unit. The following are log devices that the FortiGate unit supports:

- FortiGate system memory
- Hard disk or AMC
- SQL database (for FortiGate units that have a hard disk)
- FortiAnalyzer unit
- FortiCloud service
- Syslog server

These log devices, except for the FortiGate system memory and local hard disk, can also be used as a backup solution. For example, you can configure logging to the FortiGate unit's local disk, but also configure logging to a FortiCloud server and archive logs to both the FortiCloud server and a FortiAnalyzer unit.

If you are formatting a disk that contains more than just logs, all information on the disk will be lost

FortiGate unit's system memory and hard disk

The FortiGate unit's system memory and hard disk can store all log types, including log archives and traffic logs. Traffic logs and log archives are larger files, and need a lot of room when being logged by the FortiGate unit.

When the system memory is full, the FortiGate unit overwrites the oldest messages, and all log messages stored in memory are cleared when the FortiGate unit restarts. By default, logging to memory is enabled. This means that most of the time you will only need to modify the default settings to your network logging requirements. Real-time logging occurs whenever memory logging is enabled, and is enabled by default. Real-time logging means that the activity is being recorded as it happens.

All FortiGate units 100D and larger are capable of disk logging, but it is disabled by default, as it is not recommended. For flash memory-based units, constant rewrites to flash drives can reduce the lifetime and efficiency of the memory. For hard-disk units, it can affect performance under heavy strain. Therefore, disk logging must be manually enabled in the CLI under `config log disk setting` to appear in the interface at all.

Models without a hard disk are not recommended for disk logging. For all units, disk logging must be enabled in the CLI. For some low-end and older models, disk logging is unavailable. Check a product's Feature Matrix for more information. In either case, Fortinet recommends using either a FortiAnalyzer unit or the FortiCloud service.

When logging to the FortiGate unit's hard disk or memory, you can also configure logging to a FortiAnalyzer unit as well as upload logs to it at a scheduled time.

If you are registered with the FortiCloud service, your unit will log both locally and to the service by default. In order to configure the rate and time of uploads to the service, you must register a contract account for the FortiCloud service, which will also grant you additional space.

FortiAnalyzer unit

The FortiAnalyzer unit can log all FortiGate features, which includes log archives. You can also configure the FortiGate unit to upload logs to the FortiAnalyzer unit at a scheduled time.

Encryption of the logs is supported by default and logs are sent using IPsec or SSL VPN. When the FortiAnalyzer and FortiGate units have SSL encryption, both must choose a setting for the enc-algorithm command (CLI) for encryption to take place. By default, this is enabled and the default setting is a SSL communication with high and medium encryption algorithms. The setting that you choose must be the same for both.

FortiGate units can support logging to multiple FortiAnalyzer units. This logging solution is a backup redundancy solution, since logs are sent to all three units and whenever one of the FortiAnalyzer units fails, the others still carry on storing logs.

If you are using evaluation software FortiGate and FortiAnalyzer-VM images, you will only be able to use low-level encryption.

The FortiGate unit can also connect to a FortiAnalyzer unit using Automatic Discovery. Automatic Discovery is a method of establishing a connection to a FortiAnalyzer unit by using the FortiGate unit to find a FortiAnalyzer unit on the network. The Fortinet Discovery Protocol (FDP) is used to located the FortiAnalyzer unit. Both the FortiGate and FortiAnalyzer units must be on the same subnet to use FDP, and they must also be able to connect using UDP.

When you enable automatic discovery in the CLI, the FortiGate unit uses HELLO packets to locate any FortiAnalyzer units that are available on the network within the same subnet. When the FortiGate unit discovers a FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer unit and begins sending log data.

Syslog server

The Syslog server is a remote computer running syslog software. Syslog is a standard for forwarding log messages in an IP network, and can be used when considering a log backup solution for your network logging requirements.

FortiGate units support the reliable syslog feature, which is based on RFC 3195. Reliable syslog logging uses TCP, which ensures that connections are set up, including that packets are transmitted.

There are several profiles available for reliable syslog, but only the RAW profile is currently supported on the FortiGate units. The RAW profile is designed to provide a high-performance, low-impact footprint using essentially the same format as the existing UDP-based syslog service. The reliable syslog feature is available on FortiGate units running FortiOS 4.0 MR1 and higher.

When enabling the reliable syslog (available only in the CLI), TCP is used. The feature is disabled by default, and when enabled, the FortiGate unit automatically changes the port number to TCP 601. This is based on RFC 3195. The default port for syslog is port 514.

How to choose a log device for your network topology

When planning the log requirements, you must also consider your network's topology and whether archiving is required, such as if there is a legal requirement to keep a historical record of network activity. The following explains what steps to take when choosing a log device for your specific network topology.

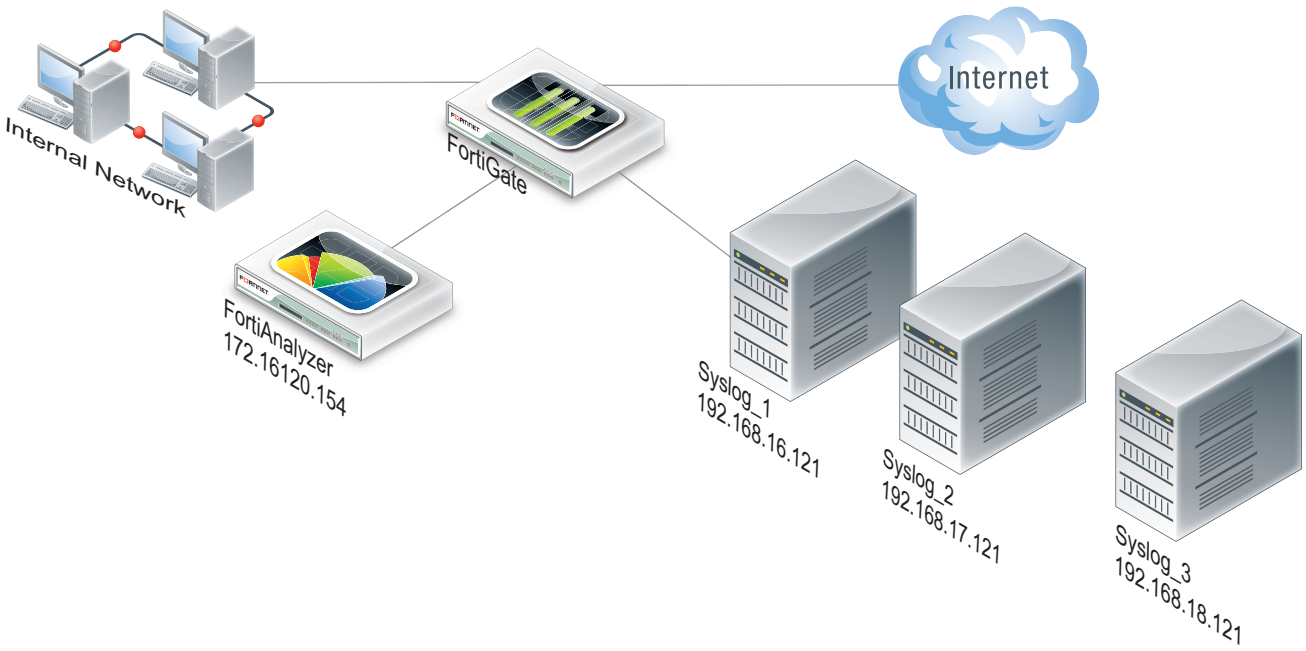
1. **What is the scope of your network topology?**
   If it is a SOHO/SMB network, then logging to the FortiGate unit's local hard disk or the default FortiCloud service would be efficient. If the network topology is a large enterprise, you will need FortiAnalyzer units, a FortiCloud contract, Syslog servers, or any combination.
2. **Is archiving required?**
   If the network activity that is being logged needs to be archived, then, depending on your network topology, you would choose a FortiAnalyzer unit. FortiAnalyzer units store archives in the same way that FortiGate units do, but are able to store large amounts of logs and archives.
3. **When troubleshooting, you may want to log a larger amount of traffic; how much storage space will you need?**
   Logs can be configured to roll, which is similar to zipping a file; this will lower the space requirements needed to contain them. You can also download logs from the FortiGate unit and save them on a server or on a computer to view and access later, to prevent them from piling up and being overwritten. If you're regularly logging large amounts of traffic, you should consider a FortiAnalyzer or FortiCloud account .
4. **Should I invest in a log device that can grow as my network grows?**
   All networks grow, so investing in a device that can grow with your network and that can be expanded is a good investment. For example, if you currently have a SOHO/SMB topology, but see growth already starting, a

FortiAnalyzer unit would be best. A FortiAnalyzer unit provides ample storage space, and you can add two more FortiAnalyzer units to access additional storage and create a redundancy log backup solution.

How to create a backup solution for logging

The following helps to explain how to create a log backup solution for a small network topology. This example has one FortiAnalyzer unit and a subscription to the FortiCloud Service.

Example of an integrated FortiAnalyzer unit and Syslog servers in a network



1. Log in to the CLI and modify what features will be logged to the FortiAnalyzer unit as well as the settings to the default log device, the FortiGate unit's hard drive.
   By default, the FortiGate unit logs to either the system memory or hard drive, whichever is available on the FortiGate unit. Low-end FortiGate units may have logging disabled by default.
2. In the CLI, use the `config log fortianalyzer setting` command to configure logging to the FortiAnalyzer unit.
   You can only configure log settings for the FortiAnalyzer unit in the CLI. Configuring to upload logs to a FortiAnalyzer unit can be configured in both the CLI and web-based manager.
3. In the CLI, configure the settings for the Syslog server; also enable reliable syslog as well.
   Reliable syslog verifies that logs are sent to the syslog server. When you enable this setting, the default port becomes port 601.

Reports

Reports provide a way to analyze log data without manually going through a large amount of logs to get to the information you need. This section explains how to configure a FortiOS report and how to modify the existing default FortiOS Security Features report. The FortiOS default Security Features report is a report that gathers security feature activity information and compiles it into a report. This section also explains how to view these reports.

Reports provide a clear, concise overview of what is happening on your network based on log data, without manually going through large amounts of logs. Reports can be configured on a FortiGate unit or a FortiAnalyzer unit. However, in this document only FortiOS reports are explained. FortiOS reports are the reports that are generated on the FortiGate unit. FortiAnalyzer reports are configured on a FortiAnalyzer unit and for information about those reports, see the FortiAnalyzer Administration Guide.

Disk or memory logging must be enabled for reporting to be enabled. Local Reporting can then be enabled in **Log & Report > Log Settings,** in order to view and edit reports.

What are FortiOS reports?

FortiOS reports are configured from logs stored on the FortiGate unit's hard drive. These reports, generated by the FortiGate unit itself, provide a central location for both configuring and generating reports. A default FortiOS report, called the FortiGate Security Feature Daily Activity Report, is available for you to modify to your requirements. The default report provides a way to quickly and easily set up your own report from within the web-based manager. The default FortiOS report is a report that compiles security feature activity from various security-related logs, such as virus and attack logs.

FortiOS reports consist of multiple parts, regardless of whether its the default FortiOS report or a report that you have configured from scratch, and these parts are configured separately and added to the layout. These parts of a FortiOS report are:

- charts (including datasets within the charts themselves)
- themes (including styles which are within the themes themselves)
- images
- layout

The parts of a FortiOS report

Charts are used to display the log information in a clear and concise way using graphs and tables. Charts contain datasets, which are SQLite queries that help the FortiGate unit to add specific log information into the chart using the log information that is stored in the SQLite database on the local hard disk. If you want to configure a chart, you must configure the dataset first. Datasets are required for each chart, and if there is no dataset included in a chart, the chart will not be saved.

Themes provide a one-step style application for report layouts. Themes contain various styles, including styles for the table of contents, headings, headers and footers, as well as the margins of the report's pages. Themes are applied to layouts. The styles that are applied to themes are configured separately in the CLI.

You can easily upload your company or organization's logo to use within a report. By uploading your company or organization's logo and applying it to a report, you provide a personalized report that is recognizable as your company or organization's report. The image must be in JPEG, JPG or PNG format.

Layouts provide a way to incorporate the charts, images, and themes that are configured to create a formatted report. A layout is used as a template by the FortiGate unit to compile and then generate the report. The layout is also coded in the CLI.

What you can do with the default FortiOS report

You can reset the reports you have configured, as well as the default FortiOS report you modified, to default settings. When you reset reports to default settings, any configured reports that you created from scratch are lost. The `execute report-config reset` command resets the reports to default settings. If you are going to

reset the reports to their default settings, you should back up the current configuration file before doing so, in the event you want to revert back to the reports you previously created and/or modified.

The default FortiOS report can be modified so that it meets your requirements for a report. This default report is located in **Log & Report > Report > Local**. Select **Customize** to edit it.

The FortiOS default report contains several pages, which appear as stacked boxes in the editing interface. Each page contains one or multiple charts (depending on the configuration of that page in the interface), and each page in the finished report will contain information about the FortiGate unit at the top of each section.

You can select **Run Now** on the **Local** page to immediately create a report with the current layout and design. More complex reports may take longer to generate. After generating a report, you can view it by selecting it from the list below **Run Now**. Historical reports will be marked as 'Scheduled' if created automatically, or 'On Demand' if created by selecting **Run Now**.

How to modify the default FortiOS report

The following is a sample modification of the default FortiOS report, which includes adding an image.

1. In **Log & Report > Report > Config**, modify the page by adding a new Chart, which will appear on its own page in the final report.
2. Add an information Text field below the chart.
   You should always save the changes you make by selecting **Save**; otherwise, the changes you just made will be lost.
3. Modify the header to add the company's image.
   The company's image will appear in all headers throughout the report. If you select **Save** now, it will appear on all the report's pages.
4. Add other charts to the list so they will appear within the report.
   Charts marked as 'FortiGate Security Feature Security Analysis Report' are autogenerated and take up an entire page or multiple pages on their own. All other charts take up half a page, so two consecutive charts will appear on the same page in the report.
5. Modify the report settings so that the report is generated every Monday at 6 pm, and is emailed to specific employees in the company.
   Reports can be sent to others after the report has been generated, if Messaging Servers are configured.
6. Test the report's modified settings, by selecting **Run Now** in the Config page; after it is generated, go to **Log & Report > Report > Local** and view the report.
   You can tell that it has been generated because the Bandwidth Usage page's charts will be populated, and the text added below each chart appears as well.

Best Practices: Log management

When the FortiGate unit records FortiGate activity, valuable information is collected that provides insight into how to better protect network traffic against attacks, including misuse and abuse. There is a lot to consider before enabling logging on a FortiGate unit, such as what FortiGate activities to enable and which log device is best suited for your network's logging needs. A plan can help you in deciding the FortiGate activities to log, a log device, as well as a backup solution in the event the log device fails.

This plan should provide you with an outline, similar to the following:

- what FortiGate activities you want and/or need logged (for example, security features)
- the logging device best suited for your network structure

- if you want or require archiving of log files
- ensuring logs are not lost in the event a failure occurs.

After the plan is implemented, you need to manage the logs and be prepared to expand on your log setup when the current logging requirements are outgrown. Good log management practices help you with these tasks.

Log management practices help you to improve and manage logging requirements. Logging is an ever-expanding tool that can seem to be a daunting task to manage. The following management practices will help you when issues arise, or your logging setup needs to be expanded.

1. Revisit your plan on a yearly basis to verify that your logging needs are being met by your current log setup. For example, your company or organization may require archival logging, but not at the beginning of your network's lifespan. Archival logs are stored on a FortiGate unit's local hard drive, a FortiAnalyzer unit, or a FortiCloud server, in increasing order of size.
2. Configure an alert message that will notify you of activities that are important to be aware about. For example: if a branch office does not have a FortiGate administrator, you will need to know at all times that the IPsec VPN tunnel is still up and running. An alert email notification message can be configured to send only if IPsec tunnel errors occur.
3. If your organization or company uses peer-to-peer programs such as Skype or other instant messaging software, use the Applications FortiView dashboard, or the Executive Summary's report widget (Top 10 Application Bandwidth Usage Per Hour Summary) to help you monitor the usage of these types of instant messaging software. These widgets can help you in determining how these applications are being used, including if there is any misuse and abuse. Their information is taken from application log messages; however, application log messages should be viewed as well since they contain the most detailed information.
4. Ensure that your backup solution is up-to-date. If you have recently expanded your log setup, you should also review your backup solution. The backup solution provides a way to ensure that all logs are not lost in the event that the log device fails or issues arise with the log device itself.

Logging and reporting for small networks

This section explains how to configure the FortiGate unit for logging and reporting in a small office or SOHO/SMB network. To properly configure this type of network, you will be modifying the default log settings, as well as the default FortiOS report.

The following procedures are examples and can be used to help you when configuring your own network's log topology. Since some of these settings must be modified or enabled or disabled in the CLI, it is recommended to review the FortiGate CLI Reference for any additional information about the commands used herein, as well as any that you would need to use in your own network's log topology.

Modifying default log device settings

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled, except for traffic logging. The default logging location will be either the FortiGate unit's system memory or hard disk, depending on the model. Units with a flash disk are not recommended for disk logging.

Modifying the FortiGate unit's system memory default settings

When the FortiGate unit's default log device is its system memory, the following is modified for a small network topology. The following is an example of how to modify these default settings.

To modify the default system memory settings

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log memory setting
   set ips-archive disable
   set status enable
end
```

3. The following example command syntax modifies which FortiGate features that are enabled for logging:

```
config log memory filter
   set attack enable
   set forward-traffic enable
   set local-traffic enable
   set netscan enable
   set email-log-imap disable
   set multicast-traffic enable
   set scanerror enable
   set app-ctrl enable
end
```

Modifying the FortiGate unit's hard disk default settings

When the FortiGate unit's default log device is its hard disk, you need to modify those settings to your network's logging needs so that you can effectively log what you want logged. The following is an example of how to modify these default settings.

To modify the default hard disk settings

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log disk setting
   set ips-archive disable
   set status enable
   set max-log-file-size 1000
   set storage FLASH
   set log-quota 100
   set report-quota 100
end
```

3. In the CLI, enter the following to disable certain event log messages that you do not want logged:

```
config log disk filter
   set sniffer-traffic disable
   set local-traffic enable
end
```

Testing sending logs to the log device

After modifying both the settings and the FortiGate features for logging, you can test that the modified settings are working properly. This test is done in the CLI.

To test sending logs to the log device

1. In the CLI, enter the following command syntax:

```
diag log test
```

When you enter the command, the following appears:

```
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating netscan log messages with level - notice
generating a VOIP event message with level - information
generating a DNS event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a NAC QUARANTINE message with level - notification
generating a URL block message with level - warning
```

2. In the web-based interface, go to **Log & Report > Event Log > User**, and view the logs to see some of the recently generated test log messages.
   You will be able to tell the test log messages from real log messages because they do not have “real” information; for example, the test log messages for the vulnerability scan contain the destination IP address of 1.1.1.1 or 2.2.2.2.

Configuring the backup solution

A backup solution provides a way to ensure logs are not lost. The following backup solution explains logging to a FortiCloud server and uploading logs to a FortiAnalyzer unit. With this backup solution, there can be three simultaneous storage locations for logs, the first being the FortiGate unit itself, the FortiAnalyzer unit and then the FortiCloud server.

Configuring logging to a FortiCloud server

The FortiCloud server can be used as a redundant backup, or your primary logging solution. The following assumes that this service has already been registered, and a subscription has been purchased for expanded space. The following is an example of how to these settings are configured for a network’s log configuration. You need to have access to both the CLI and the web-based manager when configuring uploading of logs. The upload time and interval settings can be configured in the web-based interface.

To configure logging to the FortiCloud server

1. Go to **System > Dashboard > Status** and click **Login** next to **FortiCloud** in the **License Information** widget.
2. Enter your username and password, and click **OK**. (Or register, if you have not yet done so.)
3. Logs will automatically be uploaded to FortiCloud as long as your FortiGate is linked to your FortiCloud account.
4. To configure the upload time and interval, go to **Log & Report > Log Config > Log Settings**.
5. Under the Logging and Archiving header, you can select your desired upload time.

With FortiCloud you can easily store and access FortiGate logs that can give you valuable insight into the health and security of your network.

Configuring uploading logs to the FortiAnalyzer unit

The logs will be uploaded to the FortiAnalyzer unit at a scheduled time. The following is an example of how to upload logs to a FortiAnalyzer unit.

To upload logs to a FortiAnalyzer unit

1. Go to **Log & Report > Log Config > Log Settings**.
2. In the **Logging and Archiving** section, select the check box beside **Send Logs to FortiAnalyzer/FortiManager.**
3. Select **FortiAnalyzer (Daily at 00:00)**.
4. Enter the FortiAnalyzer unit’s IP address in the **IP Address** field.
5. To configure the daily upload time, open the CLI.
6. Enter the following to configure when the upload occurs, and the time when the unit uploads the logs:

```
config log fortianalyzer setting
   set upload-interval {daily | weekly | monthly}
   set upload-time <hh:mm>
end
```

7. To change the upload time, in the web-based manager, select **Change** beside the upload time period, and then make the changes in the Upload Schedule window. Select **OK**.

Testing uploading logs to a FortiAnalyzer unit

You should test that the FortiGate unit can upload logs to the FortiAnalyzer unit, so that the settings are configured properly.

To test the FortiAnalyzer upload settings

1. Go to **Log & Report > Log Config > Log Settings.**
2. In the **Logging and Archiving** section, under **Send Logs to FortiAnalyzer/FortiManager**, change the time to the current time by selecting **Change**.
   For example, the current time is 11:10 am, so **Change** now has the time 11:10.
3. Select **OK**.

The logs will be immediately sent to the FortiAnalyzer unit, and will be available to view from within the FortiAnalyzer's interface.

Modifying the default FortiOS report

The default FortiOS report is provided to help you quickly and easily configure and generate a report. The following is an example of how to modify the default FortiOS report.

To modify the default FortiOS report

1. In the web-based manager, go to **Log & Report > Report > Local**.
2. Select **Customize** to open the Report Editor.
3. Change the default Fortinet image to the new image: select the Fortinet image and right-click so that **Delete** icon appears, and then select **Delete**; drag the Image icon to the box where the Fortinet image was previous; choose or upload a new image and then select **OK**.
4. Return to **Log & Report > Report > Local**.
5. Under **Report Options**, set the Generate report schedule to **Daily** and set a Time for the report to be compiled every day.
6. Enable **Email Generated Reports**. You may have to configure an SMTP server to send the reports before this option can be enabled. The SMTP configuration can be found in **System > Config > Messaging Servers**.
7. Select **Apply** to save the changes.
8. Select **Run Now** to generate a new On Demand report based on your changes.
9. Select the report from the Historical Reports list to view it.

Running On Demand reports can be a good way to compare report modifications as you configure.

Logging and reporting for large networks

This section explains how to configure the FortiGate unit for logging and reporting in a larger network, such as an enterprise network. To set up this type of network, you are modifying the default log settings, and you are also modifying the default report.

The following procedures are examples and can be used to help you when configuring your own network's log topology.

Since some of these settings must be modified or enabled or disabled in the CLI, it is recommended to review the FortiGate CLI Reference for any additional information about the commands used herein, as well as any that you would need to use in your own newtork's log topology.

Modifying default log device settings

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled and well as logging to either the FortiGate unit's system memory or hard disk, depending on the model.

Modifying multiple FortiGate units' system memory default settings

When the FortiGate unit's default log device is its system memory, you can modify it to fit your log network topology. In this topic, the following is an example of how you can modify these default settings.

To modify the default system memory settings

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log memory setting
   set ips-archive disable
   set status enable
end
```

3. Enter the following command syntax to modify the FortiGate features that are enabled for logging:

```
config log memory filter
   set attack enable
   set forward-traffic enable
   set local-traffic enable
   set netscan enable
   set email-log-imap enable
   set multicast-traffic enable
   set scanerror enable
   set app-ctrl enable
end
```

4. Repeat steps 2 and 3 for the other FortiGate units.
5. Test the modified settings using the procedure below.

Modifying multiple FortiGate units' hard disk default log settings

You will have to modify each FortiGate unit's hard disk default log settings. The following is an example of how to modify these default settings.

To modify the default hard disk settings

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log disk setting
   set ips-archive disable
   set status enable
   set max-log-file-size 1000
   set storage Internal
   set log-quota 100
   set report-quota 100
end
```

3. In the CLI, enter the following to disable certain event log messages that you do not want logged:

```
config log disk filter
   set sniffer-traffic disable
   set local-traffic enable
end
```

4. Repeat the steps 2 to 4 for the other FortiGate units.
5. Test the modified settings using the procedure below.

Testing the modified log settings

After modifying both the settings and the FortiGate features for logging, you can test that the modified settings are working properly. This test is done in the CLI.

To test sending logs to the log device

1. In the CLI, enter the following command syntax:

```
diag log test
```

When you enter the command, the following appears:

```
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
```

```
generating netscan log messages with level - notice
generating a VOIP event message with level - information
generating a DNS event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a NAC QUARANTINE message with level - notification
generating a URL block message with level - warning
```

2. In the web-based interface, go to **Log & Report > Event Log > User**, and view the logs to see some of the recently generated test log messages.
   You will be able to tell the test log messages from real log messages because they do not have “real” information; for example, the test log messages for the vulnerability scan contain the destination IP address of 1.1.1.1 or 2.2.2.2.

Configuring the backup solution

Even though you are logging to multiple FortiAnalyzer units, this is more of a redundancy solution rather than a complete backup solution in this example.

The multiple FortiAnalyzer units act similar to a HA cluster, since if one FortiAnalyzer unit fails, the others continue storing the logs they receive. In a backup solution, the logs are backed up to another secure location if something happens to the log device.

A good alternate or redundant option is the FortiCloud service, which can provide secure online logging and management for multiple devices.

Configuring logging to multiple FortiAnalyzer units

The following example shows how to configure logging to multiple FortiAnalyzer units. Configuring multiple FortiAnalyzer units is quick and easy; however, you can only configure up to three FortiAnalyzer units per FortiGate unit.

To configure multiple FortiAnalyzer units

1. In the CLI, enter the following command syntax to configure the first FortiAnalyzer unit:

```
config log fortianalyzer setting
   set status enable
   set server 172.20.120.22
   set max-buffer-size 1000
   set buffer-max-send 2000
   set address-mode static
   set conn-timeout 100
   set monitor-keepalive-period 120
   set monitor-failure-retry-period 2000
end
```

2. Disable the features that you do not want logged, using the following example command syntax. You can view the CLI Reference to see what commands are available.

```
config log fortianalyzer filter
   set traffic (enable | disable)
   ...
end
```

3. Enter the following commands for the second FortiAnalyzer unit:

```
   config log fortianalyzer2 setting
      set status enable
      set server 172.20.120.23
      set max-buffer-size 1000
      set buffer-max-send 2000
      set address-mode static
      set conn-timeout 100
      set monitor-keepalive-period 120
      set monitor-failure-retry-period 2000
end
```

4. Disable the features that you do not want logged, using the following example command syntax.

```
config log fortianalyzer filter
   set web (enable | disable)
   ...
end
```

5. Enter the following commands for the last FortiAnalyzer unit:

```
   config log fortianalyzer3 setting
      set status enable
      set server 172.20.120.23
      set max-buffer-size 1000
      set buffer-max-send 2000
      set address-mode static
      set conn-timeout 100
      set monitor-keepalive-period 120
      set monitor-failure-retry-period 2000
end
```

6. Disable the features that you do not want logged, using the following example command syntax.

```
config log fortianalyzer filter
   set web-filter (enable | disable)
   ...
end
```

7. Test the configuration by using the procedure, "Testing the modified log settings".
8. On the other FortiGate units, configure steps 1 through 6, ensuring that logs are being sent to the FortiAnalyzer units.

Configuring logging to the FortiCloud server

The FortiCloud server can be used as a redundant backup, or your primary logging solution. The following assumes that this service has already been registered, and a subscription has been purchased for expanded space. The following is an example of how to these settings are configured for a network's log configuration. You need to have access to both the CLI and the web-based manager when configuring uploading of logs. The upload time and interval settings can be configured in the web-based interface.

To configure logging to the FortiCloud server

1. Go to **System > Dashboard > Status** and click **Login** next to **FortiCloud** in the License Information widget.
2. Enter your username and password, and click **OK**. (Or register, if you have not yet done so.)
3. Logs will automatically be uploaded to FortiCloud as long as your FortiGate is linked to your FortiCloud account.
4. To configure the upload time and interval, go to **Log & Report > Log Config > Log Settings**.

5. Under the Logging and Archiving header, you can select your desired upload time.
6. With FortiCloud you can easily store and access FortiGate logs that can give you valuable insight into the health and security of your network.

Modifying the default FortiOS report

The default FortiOS report is provided to help you quickly and easily configure and generate a report. Below is a sample configuration with multiple examples of significant customizations that you can make to tailor reports for larger networks.

Creating datasets

You need to create a new dataset for gathering information about HA, admin activity and configuration changes.

Creating datasets requires SQL knowledge.

To create the datasets

1. Log in to the CLI.
2. Enter the following command syntax:

```
config report dataset
   edit ha
      set query "select subtype_ha count(*) as totalnum from event_log
         where timestamp >= F_TIMESTAMP ('now', 'hour', '-23') and group by subtype_ha
            order by totalnum desc"
      next
```

3. Create a dataset for the admin activity, that includes log ins and log outs from the three FortiGate administrators.

```
      set query "select subtype_admin count(*) as totalnum from event_log
         where timestamp >= F_TIMESTAMP ('now', 'hour', '-23') and group by subtype_
            admin order by totalnum desc"
      next
```

4. Create a dataset for the configuration changes that the administrators did for the past 24 hours.

```
      set query "select subtype_config count(*) as totalnum from event_log
         where timestamp >= F_TIMESTAMP ('now', 'hour', '-23') and group by subtype_
            config order by totalnum desc"
      next
end
```

Creating charts for the datasets

1. Log in to the CLI.
2. Enter the following to create a new chart:

```
config report chart
   edit ha.24h
      set type table
      set period last24h
      set dataset ha
      set category event
      set favorite no
```

```
    set style auto
    set title "24 Hour HA Admin Activity"
end
```

Uploading the corporate images

You need to upload the corporate images so that they appear on the report's pages, as well as on the cover page. Uploading images is only available in the web-based manager.

To upload corporate images

1. Go to **Log & Report > Report > Local**.
2. Select the Image icon and drag it to a place on the page.
3. The Graphic Chooser window appears.
4. Select Upload and then locate the image that you want to upload and upload the image.
   The images are automatically uploaded and saved.
5. Repeat step 4 until the other corporate images are uploaded.
6. Select Cancel to close the Graphic Chooser window and return to the page.

The images can then be placed as you like by reopening the Graphic Chooser as in step 2.

Adding a new report cover and page

You need to add a new cover for the report, as well as a new page that will display the HA activity, admin activity and configuration changes.

To add and customize a new report cover

1. Go to **Log & Report > Report > Local**.
2. Select **Customize**.
3. In **Sections**, select the current default report section, and enter `Report Cover` in the field that appears; then press Enter to save the change.
4. Remove all content from the Report Cover section, and select the image icon and drag it into the main portion of the cover page; select a cover page image and then select **OK**.
5. Select the font size you want, and drag the text icon into the area beneath the image to add a title or explanation for the cover page.
6. Select **Save** to save the new report cover.

To add and customize a new page

1. Go to **Log & Report > Report > Local**.
2. Select **Customize**.
3. Select **Sections**, and select **Create New** to add a new section to the report. Name it `Report Content`, and press **Enter**, and **OK** to close the menu.
4. At the bottom of the editing window is the **Section** selection, where each **Section** is represented by a box. Select the second box.
5. Edit the content for the report as you like.
   For a simpler report structure, make use of the 'FortiGate UTM Security Analysis Report' charts, which automatically format themselves and fill in all necessary information.
   For more complex reports, add headings, default and custom charts, and explanatory text.

6. Select **Save** to save the new report content.
   The report will automatically combine all sections. You can use headers and text to more clearly separate parts of the report, and all properly configured charts have titles built-in.

Advanced logging

This section explains how to configure other log features within your existing log configuration. You may want to include other log features after initially configuring the log topology because the network has either outgrown the initial configuration, or you want to add additional features that will help your network's logging requirements.

The following topics are included in this section:

- Configuring logging to multiple Syslog servers
- Using Automatic Discovery to connect to a FortiAnalyzer unit
- Activating a FortiCloud account for logging purposes
- Viewing log storage space
- Customizing and filtering log messages
- Viewing logs from the CLI
- Configuring NAC quarantine logging
- Logging local-in policies
- Tracking specific search phrases in reports
- Reverting modified report settings to default settings

Configuring logging to multiple Syslog servers

When configuring multiple Syslog servers (or one Syslog server), you can configure reliable delivery of log messages from the Syslog server. Configuring of reliable delivery is available only in the CLI.

If VDOMs are enabled, you can configure multiple FortiAnalyzer units or Syslog servers for each VDOM.

To enable logging to multiple Syslog servers

1. Log in to the CLI.
2. Enter the following commands:

```
config log syslogd setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

3. Enter the following commands to configure the second Syslog server:

```
config log syslogd2 setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

4. Enter the following commands to configure the third Syslog server:

```
config log syslogd3 setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

Most FortiGate features are, by default, enabled for logging. You can disable individual FortiGate features you do not want the Syslog server to record, as in this example:

```
config log syslogd filter
   set traffic {enable | disable}
   set web {enable | disable}
   set url-filter {enable | disable}
end
```

Using Automatic Discovery to connect to a FortiAnalyzer unit

Automatic Discovery can be used if the FortiAnalyzer unit is on the same network.

To connect using automatic discovery

1. Log in to the CLI.
2. Enter the following command syntax:

```
config log fortianalyzer setting
   set status enable
   set server <ip_address>
   set gui-display enable
   set address-mode auto-discovery
end
```

If your FortiGate unit is in Transparent mode, the interface using the automatic discovery feature will not carry traffic. For more information about how to enable the interface to also carry traffic when using the automatic discovery feature, see the Fortinet Knowledge Base article, Fortinet Discovery Protocol in Transparent mode.

The FortiGate unit searches within the same subnet for a response from any available FortiAnalyzer units.

Activating a FortiCloud account for logging purposes

When you subscribe to FortiCloud, you can configure to send logs to the FortiCloud server. The account activation can be done within the web-based manager, from the **License Information** widget located in **System > Dashboard**.

From this widget, you can easily create a new account, or log in to the existing account. From within the License Information widget, after the account is activated, you can go directly to the FortiCloud web portal, or log out of the service if you are already logged in.

To activate a FortiCloud account for logging purposes:

The following assumes that you are already at **System > Dashboard** and that you have located the License Information widget.

1. In the License Information widget, select **Activate** in the **FortiCloud** section.
   The Registration window appears. From this window, you create the login credentials that you will use to access the account.
2. Select **Create Account** and enter then information for the login credentials.
   After entering the login credentials, you are automatically logged in to your FortiCloud account.
3. Check that the account has been activated by viewing the account status from the License Information widget.

If you need more space, you can subscribe to the 200Gb FortiCloud service by selecting **Upgrade** in the **FortiCloud** section of the widget.

Viewing log storage space

The `diag sys logdisk usage` command allows you to view detailed information about how much space is currently being used for logs. This is useful when you see a high percentage, such as 92 percent for the disk's capacity. The FortiGate unit uses only 75 percent of the available disk capacity to avoid a high storage amount so when there is a high percentage, it refers to the percentage of the 75 percent that is available. For example, 92 percent of the 75 percent is available.

The following is an example of what you may see when you use `diag sys logdisk usage` command on a unit with no VDOMs configured:

```
diag sys logdisk usage
```

The following appears:

```
Total HD usage: 176MB/3011 MB
Total HD logging space: 22583MB
Total HD logging space for each vdom: 22583MB
HD logging space usage for vdom "root": 30MB/22583MB
```

Customizing and filtering log messages

When viewing log messages, you may want to customize and filter the information that you are seeing in the Log & Report menu (for example, Log & Report > Traffic Log > Forward Traffic). Filtering and customizing the display provides a way to view specific log information without scrolling through pages of log messages to find the information.

Customizing log messages is the process of removing or adding columns to the log display page, allowing you to view certain desired information. The most columns represent the fields from within a log message, for example, the user column represents the user field, as well as additional information. If you want to reset the customized columns on the page back to their defaults, you need to select **Reset All Columns** within the column title right-click menu.

Filtering information is similar to customizing, however, filtering allows you to enter specific information that indicates what should appear on the page. For example, including only log messages that appeared on February 24, between the hours of 8:00 and 8:30 am.

To customize and filter log messages

The following is an example that displays all traffic log messages that originate from the source IP address 172.20.120.24, as well as displaying only the columns:

- OS Name
- OS Version
- Policy ID
- Src (Source IP)

The following assumes that you are already on the page of the log messages you want to customize and filter. In this example, the log messages that we are customizing and filtering are in **Log & Report > Traffic Log > Forward Traffic**.

1. On the Forward Traffic page, right click anywhere on a column title.
2. Right click on a column title, and mouse over **Column Settings** to open the list.
3. Select each checkmarked title to uncheck it and remove them all from the displayed columns.
4. Scroll down to the list of unchecked fields and select 'OS Name', 'OS Version', 'Policy ID', and 'Src' to add checkmarks next to them.
5. Click outside the menu, and wait for the page to refresh with the new settings in place.
6. Select the funnel icon next to the word Src in the title bar of the Src column.
7. Enter the IP you want displayed (in this example, 172.20.120.24) in the text box.
8. Click **Apply**, and wait for the page to reload.

Viewing logs from the CLI

You can easily view log messages from within the CLI. In this example, we are viewing DLP log messages.

1. Log in to the CLI and then enter the following to configure the display of the DLP log messages.

   ```
   execute log filter category 9
   execute log filter start-line 1
   execute log filter view-lines 20
   ```

   The customized display of log messages in the CLI is similar to how you customize the display of log messages in the web-based manager. For example, `category 9` is the DLP log messages, and the `start-line` is the first line in the log database table for DLP log messages, and there will be 20 lines (`view-lines 20`) that will display.

2. Enter the following to view the log messages:

   ```
   execute log display
   ```

   The following appears below execute log display:

   ```
   600 logs found
   20 logs returned
   ```

   along with the 20 DLP log messages.

Configuring NAC quarantine logging

NAC quarantine log messages provide information about what was banned and quarantined by a Antivirus profile. The following explains how to configure NAC quarantine logging and enable it on a policy. This procedure assumes the Antivirus profile is already in place.

To configure NAC quarantine logging

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select the policy that you want to apply the Antivirus profile to, and then select **Edit**.
3. Within the Security Profiles section, enable **Antivirus** and then select the profile from the drop-down list.
4. Select **OK**.
5. Log in to the CLI.
6. Enter the following to enable NAC quarantine in the DLP sensor:

```
config antivirus profile
   edit <profile_name>
      config nac-quar log enable
   end
```

Logging local-in policies

Local-in security policies are policies the control the flow of internal traffic, and can be used to broaden or restrict an administrator's access privileges. These local-in policies can also be configured to log traffic and activity that the policies control.

You can enable logging of local-in policies in the CLI, with the following commands:

```
config system global
   set gui-local-in-policy enable
end
```

The Local-In Policy page will then be available in **Policy & Objects > Policy > Local In**. You can configure what local-in traffic to log in the CLI, or in **Log & Report > Log Config > Log Settings**, under **Local Traffic Logging**.

When deciding what local-in policy traffic you want logged, consider the following:

Special Traffic

Traffic activity	Traffic Direction	Description
FortiGuard update annouce-ments	IN	All push announcements of updates that are coming from the FortiGuard system. For example, IPS or AV updates.
FortiGuard update requests	OUT	All updates that are checking for antivirus or IPS as well as other FortiGuard service updates.
Firewall authen-tication	IN	The authentication made using either the web-based manager or CLI.
Central man-agement (a FortiGate unit being managed by a FortiMan-ager unit)	IN	The access that a FortiManager has managing the FortiGate unit.
DNS	IN	All DNS traffic.
DHCP/DHCP Relay	IN	All DHCP and/or DHCP Relay traffic.
HA (heart beat sync policy)	IN/OUT	For high-end platforms with a backplane heart beat port.
HA (Session sync policy)	IN/OUT	This will get information from the CMDB and updated by session sync daemon.
CAPWAP	IN	This activity is logged only when a HAVE_CAPWAP is defined.
Radius	IN	This is recorded only within FortiCarrier.
NETBIOS forward	IN	Any interface that NETBIOS forward is enabled on.
RIP	IN	
OSPF	IN	
VRRP	IN	
BFD	IN	
IGMP	IN	This is recorded only when PIM is enabled.
PIM	IN	This is recorded only when PIM is enabled.
BGP	IN	This is recorded only when config bgp and bgp neightbor is enabled in the CLI.

Traffic activity	Traffic Direction	Description
WCCP policy	IN	Any interface that WCCP is enabled; however, if in Cache mode, this is not recorded because it is not available.
WAN Opt/ Web Cache	IN	Any interface where WAN Opt is enabled.
WANOpt Tunnel	IN	This is recorded when HAVE_WANOPT is defined.
SSL-VPN	IN	Any interface from a zone where the action in the policy is SSL VPN.
IPSEC	IN	
L2TP	IN	
PPTP	IN	
VPD	IN	This is recorded only when FortiClient is enabled.
Web cache db test facility	IN	This is recorded only when WA_CS_REMOTE_TEST is defined.
GDBserver	IN	This is recorded only when debug is enabled.

Tracking specific search phrases in reports

It is possible to use the Web Filter to track specific search keywords and phrases and record the results for display in the report.

You should verify that the web filter profile you are using indicates what search phrases you want to track and monitor, so that the report includes this information.

1. **Log in to the CLI and enter show webfilter profile default.**
   This provides details about the webfilter profile being used by the security policy. In this example, the details (shown in the following in bold) indicate that safe search is enabled, but not specified or being logged.

```
show webfilter profile default
   config webfilter profile
      edit "default"
         set comment "default web filtering"
         set inspection-mode flow-based
         set options https-scan
         set post-action comfort
            config web
               set safe-search url
            end
            config ftgd-wf
               config filters
                  edit 1
                     set action block
                     set category 2
                  next
```

```
edit 2
   set action block
   set category 7
next
edit 3
   set action block
   set category 8
```

2. **Enter the following command syntax so that logging and the keyword for the safe search will be included in logging.**

```
config webfilter profile
   edit default
      config web
         set log-search enable
         set keyword-match "fortinet" "easter" "easter bunny"
      end
   end
```

3. **To test that the keyword search is working, go to a web browser and begin searching for the words that were included in the webfilter profile, such as easter.**
   You can tell that the test works by going to **Log & Report > Traffic Log > Forward Traffic** and viewing the log messages.

Reverting modified report settings to default settings

If you need to go back to the original default report settings, you can easily revert to those settings in the Report menu. Reverting to default settings means that your previously modified report settings will be lost.

To revert back to default report settings, in **Log & Report > Report > Local**, select **Customize**, and then **Restore Defaults** from the top navigation. This may take a minute or two. You can also use the CLI command `execute report-config reset` to reset the report to defaults.

If you are having problems with report content being outdated or incorrect, especially after a firmware update, you can recreate the report database using your current log information with the CLI command `execute report recreate-db`.

Troubleshooting and logging

This section explains how to troubleshoot logging configuration issues, as well as connection issues, that you may have with your FortiGate unit and a log device. This section also contains information about how to use log messages when troubleshooting issues that are about other FortiGate features, such as VPN tunnel errors.

Using log messages to help in troubleshooting issues

Log messages can help when troubleshooting issues that occur, since they can provide details about what is occurring. The uses and methods for involving logging in troubleshooting vary depending on the problem. The following are examples of how log messages can assist when troubleshooting networking issues.

Using IPS packet logging in diagnostics

This type of logging should only be enabled when you need to know about specific diagnostic information, for example, when you suspect a signature is triggered by a false positive. These log messages can help troubleshoot individual problems with misidentified or missing packets and network intrusions involving malicious packets.

To configure IPS packet logging

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the IPS sensor that you want to enable IPS packet logging on, and then select **Edit**.
3. In the filter options, enable **Packet Logging**.
4. Select **OK**.

If you want to configure the packet quota, number of packets that are recorded before alerts and after attacks, use the following procedure.

To configure additional settings for IPS packet logging

1. Log in to the CLI.
2. Enter the following to start configuring additional settings:

```
config ips settings
     set ips-packet-quota <integer>
     set packet-log-history <integer>
     set packet-log-post-attack <integer>
end
```

Using HA log messages to determine system status

When the FortiGate unit is in HA mode, you may see the following log message content within the event log:

```
type=event subtype=ha level=critical msg= "HA slave heartbeat interface internal lost
    neighbor information"
```

OR

```
type=event subtype=ha level=critical msg= "Virtual cluster 1 of group 0 detected new
    joined HA member"
```

OR

```
type=event subtype=ha level=critical msg= "HA master heartbeat interface internal get peer
    information"
```

The log messages occur within a given time, and indicate that the units within the cluster are not aware of each other anymore. These log messages provide the information you need to fix the problem.

Connection issues between FortiGate unit and logging devices

If external logging devices are not recording the log information properly or at all, the problem will likely be due to one of two situations: no data is being received because the log device cannot be reached, or no data is being sent because the FortiGate unit is no longer logging properly.

Unable to connect to a supported log device

After configuring logging to a supported log device, and testing the connection, you may find you cannot connect. To determine whether this is the problem:

1. Verify that the information you entered is correct; it could be a simple mistake within the IP address or you may have not selected **Apply** on the Log Settings page after changing them, which would prevent them from taking effect.
2. Use `execute ping` to see if you can ping to the log device.
3. If you are unable to ping to the log device, check to see if the log device itself working and that it is on the network and assigned an appropriate address.

FortiGate unit has stopped logging

If the FortiGate unit stopped logging to a device, test the connection between both the FortiGate unit and device using the execute ping command. The log device may have been turned off, is upgrading to a new firmware version, or just not working properly.

The FortiGate unit may also have a corrupted log database. When you log into the web-based manager and you see an SQL database error message, it is because the SQL database has become corrupted. View "SQL database errors" in the next section before taking any further actions, to avoid losing your current logs.

Log database issues

If attempting to troubleshoot issues with the SQL log database, use the following to help guide you to solving issues that occur.

SQL statement syntax errors

There may be errors or inconsistencies in the SQL used to maintain the database. Here are some example error messages and possible causes:

```
You have an error in your SQL syntax (remote/MySQL)
```

or

```
ERROR: syntax error at or near... (local/PostgreSQL)
```

- Verify that the SQL keywords are spelled correctly, and that the query is well-formed.
- Table and column names are demarked by grave accent (`) characters. Single (') and double (") quotation marks will cause an error.

```
No data is covered.
```

- The query is correctly formed, but no data has been logged for the log type. Verify that you have configured the FortiGate unit to save that log type. On the Log Settings page, make sure that the log type is checked.

Connection problems

If well-formed SQL queries do not produce results, and logging is turned on for the log type, there may be a database configuration problem with the remote database.

Ensure that:

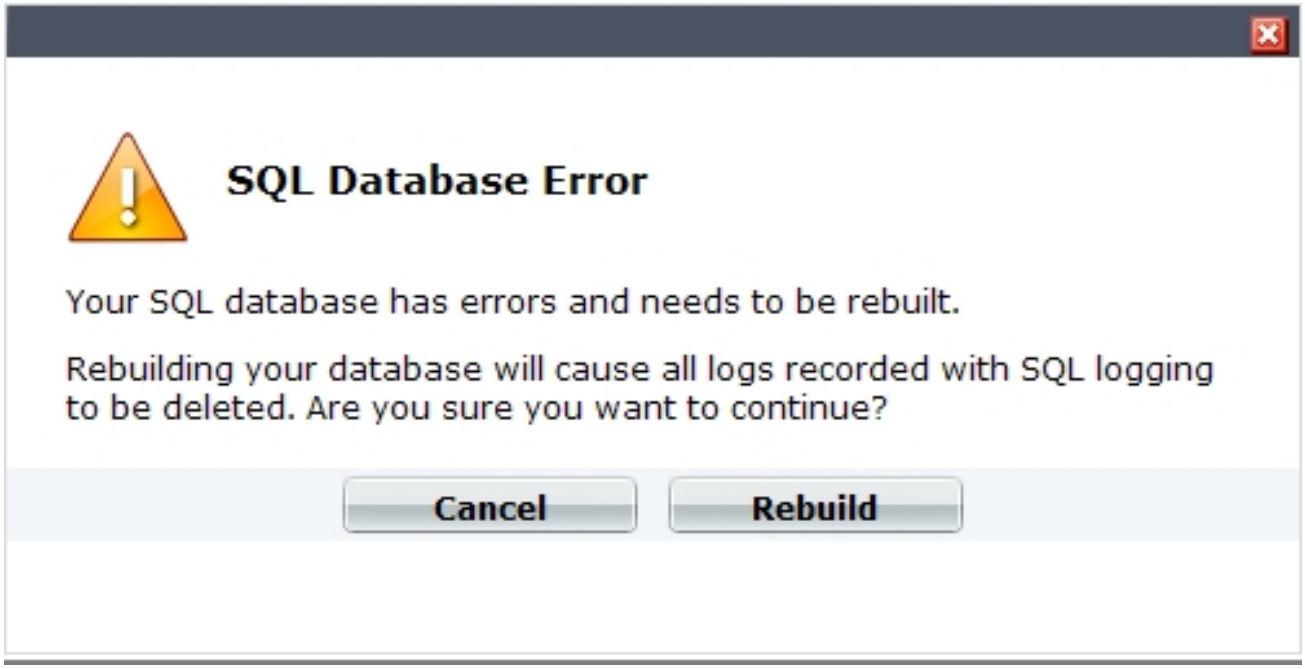
- MySQL is running and using the default port 3306.
- You have created an empty database and a user who has read/write permissions for the database.
- Here is an example of creating a new MySQL database named fazlogs, and adding a user for the database:

1. `#Mysql -u root -p`
2. `mysql>` Create database fazlogs;
3. `mysql>` Grant all privileges on fazlogs.* to 'fazlogger'@'*' identified by 'fazpassword';
4. `mysql>` Grant all privileges on fazlogs.* to 'fazlogger'@'localhost' identified by 'fazpassword';

SQL database errors

If the database seems inacessible, you may encounter the following error message after upgrading or downgrading the FortiGate unit's firmware image.

Example of an SQL database error message



The error message indicates that the SQL database is corrupted and cannot be updated with the SQL schemas any more. When you see this error message, you can do one of the following:

- select **Cancel** and back up all log files; then select **Rebuild** to blank and rebuild the database.
- select **Rebuild** immediately, which will blank the database and previous logs will be lost.

Until the database is rebuilt, no information will be logged by the FortiGate unit regardless of the log settings that are configured on the unit. When you select **Rebuild**, all logs are lost because the SQL database is erased and then rebuilt again. Logging resumes automatically according to your settings after the SQL database is rebuilt.

To view the status of the database, use the `diagnose debug sqldb-error status` command in the CLI. This command will inform you whether the database has errors present.

If you want to view the database's errors, use the `diagnose debug sqldb-error read` command in the CLI. This command indicates exactly what errors occurred, and what tables contain those errors.

Log files are backed up using the `execute backup {disk | memory } {alllogs | logs}` command in the CLI. You must use the text variable when backing up log files because the text variable allows you to view the log files outside the FortiGate unit. When you back up log files, you are really just copying the log files from the database to a specified location, such as a TFTP server.

Logging daemon (Miglogd)

The number of logging daemon child processes has been made available for editing. A higher number can affect performance, and a lower number can affect log processing time, although no logs will be dropped or lost if the number is decreased.

If you are suffering from performance issues, you can alter the number of logging daemon child processes, from 0 to 15, using the following syntax. The default is 8.

```
config system global
   set miglogd-children <integer>
end
```

Chapter 19 - Managing Devices

This handbook chapter contains the following sections:

Managing “bring your own device” describes device monitoring, devices, device groups, and device policies. The administrator can monitor all types of devices and control their access to network resources.

Endpoint Protection describes how you can enforce the use of FortiClient Endpoint Control and apply an endpoint profile to users’ devices. Endpoint profiles include real-time antivirus protection, application control, web category filtering, and VPN provisioning.

Vulnerability Scan describes how perform network vulnerability scanning to look for security weaknesses in your servers and workstations.

Managing “bring your own device”

FortiOS can control network access for different types of personal mobile devices that your employees bring onto your premises. You can:

- identify and monitor the types of devices connecting to your networks, wireless or wired
- use MAC address based access control to allow or deny individual devices
- create security policies that specify device types
- enforce endpoint control on devices that can run FortiClient Endpoint Control software

Device monitoring

The FortiGate unit can monitor your networks and gather information about the devices operating on those networks. Collected information includes:

- MAC address
- IP address
- operating system
- hostname
- user name
- how long ago the device was detected and on which FortiGate interface

You can go to **User & Device > Device > Device Definitions** to view this information. Mouse-over the **Device** column for more details.

Device monitoring is enabled separately on each interface. Device detection is intended for devices directly connected to your LAN ports. If enabled on a WAN port, device detection may be unable to determine the operating system on some devices.

To configure device monitoring

1. Go to **System > Network > Interfaces**.
2. Edit the interface that you want to monitor devices on.
3. In **Device Management**, select **Detect and Identify Devices**.
4. Select **OK**.
5. Repeat steps 2 through 4 for each interface that will monitor devices.

For ease in identifying devices, Fortinet recommends that you assign each device an Alias.

To assign an alias to a detected device or change device information

1. Go to **User & Device > Device > Device Definitions.**
2. Double-click the device entry or right-click it and select **Edit**.
3. Enter an **Alias** such as the user’s name to identify the device.
   This is step is compulsory. The alias replaces the MAC address in the device list.
4. Change other information as needed.
5. Select **OK**.

To add a device manually

1. Go to **User & Device > Device > Device Definitions** and select **Create New**.
2. Enter the following information:
   - Alias (required)
   - MAC address
   - Device Type
   - Optionally, add the device to **Custom Groups**.
   - Optionally, enter **Comments**.
3. Select **OK**.

Device Groups

You can specify multiple device types in a security policy. As an alternative, you can add multiple device types to a custom device group and include the group in the policy. This enables you to create a different policy for devices that you know than for devices in general.

To create a custom device group and add devices to it

1. Go to **User & Device > Device > Device Groups.**
   The list of device groups is displayed.
2. Select **Create New**.
3. Enter a **Name** for the new device group.
4. Click in the **Members** field and click a device type to add. Repeat to add other devices.
5. Select **OK**.

Controlling access with a MAC Address Access Control List

A MAC Address Access Control List (ACL) allows or blocks access on a network interface that includes a DHCP server. If the interface does not use DHCP, or if you want to limit network access to a larger group such as employee devices, it is better to create a device group and specify that group in your security policies.

A MAC Address ACL functions as either a list of blocked devices or a list of allowed devices. This is determined by the **Unknown MAC Address** entry.

By default, the ACL is a list of blocked devices. The **Unknown MAC Address** entry **Action** is **Assign IP**. You add an entry for each MAC address that you want to block and set its **Action** to **Block**.

If you want the ACL to allow only a limited set of devices, you set the **Unknown MAC Address** entry to **Bloc**. Then, add the MAC address of each allowed device. Set **Action** to **Assign IP**. Optionally, you can set **Action** to **Reserve** and enter the IP address that will always be assigned to the device.

To create a MAC Address ACL to allow only specific devices

1. Go to the SSID or network interface configuration.
2. In the **DHCP Server** section, expand **Advanced**.
   DHCP Server must be enabled.
3. In **MAC Reservation + Access Control,** select **Create New** and enter an allowed device’s **MAC Address**.
4. In the **IP or Action** column, select one of:
   - Assign IP — device is assigned an IP address from the DHCP server address range.
   - Reserve IP — device is assigned the IP address that you specify.
5. Repeat Steps "Managing “bring your own device”" on page 1946 and "Managing “bring your own device”" on page 1946 for each additional MAC address entry.
6. Set the **Unknown MAC Address** entry **IP or Action** to **Block**.
7. Select **OK**.

To create a MAC Address ACL to block specific devices

1. Go to the SSID or network interface configuration.
2. In the **DHCP Server** section, expand **Advanced**.
   DHCP Server must be enabled.
3. In **MAC Reservation + Access Control,** select **Create New** and enter a blocked device’s **MAC Address**.
4. In the **IP or Action** column, select **Block**.
5. Repeat Steps "Managing “bring your own device”" on page 1946 and "Managing “bring your own device”" on page 1946 for each additional MAC address entry.
6. Set the **Unknown MAC Address** entry **IP or Action** to **Assign IP**.
7. Select **OK**.

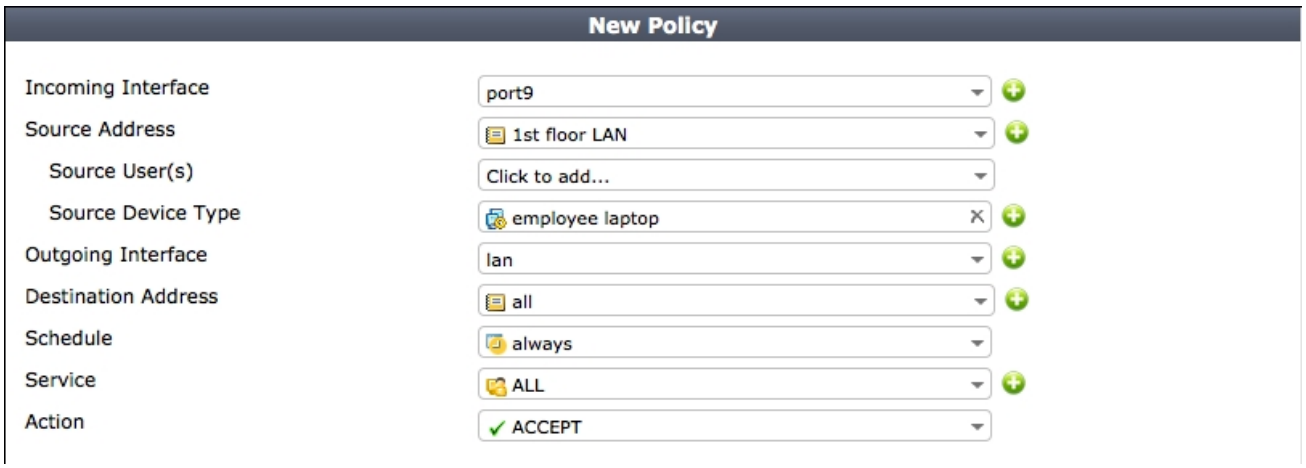
Security policies for devices

Security policies enable you to implement policies according to device type. For example:

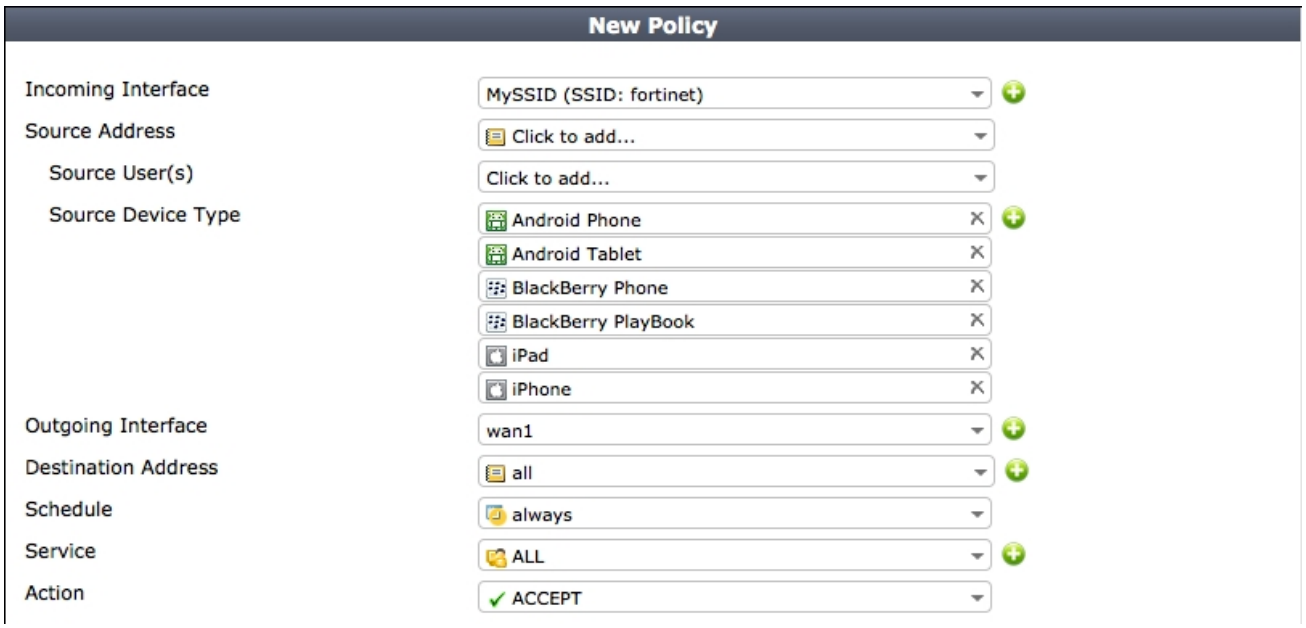
- Gaming consoles cannot connect to the company network or the Internet.
- Personal tablet and phone devices can connect to the Internet but not to company servers.
- Company-issued laptop computers can connect to the Internet and company servers. Web filtering and antivirus are applied.
- Employee laptop computers can connect to the Internet, but web filtering is applied. They can also connect to company networks, but only if FortiClient Endpoint Security is installed to protect against viruses.

The following images show these policies implemented for WiFi to the company network and to the Internet.

Device policies for company laptop access to the company network



Device policies for WiFi access to the Internet



The next section explains device policy creation in detail.

Creating device policies

Device-based security policies are similar to policies based on user identity:

- The policy enables traffic to flow from one network interface to another.
- NAT can be enabled.
- UTM protection can be applied.

To create a device policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Choose **Incoming Interface**, **Source Address**, and **Outgoing Interface** as you would for any security policy.
3. In Source Device Type, select the device types that can use this policy.
   You can select multiple devices or device groups.
4. Select **Enable NAT** if appropriate.
5. Configure **UTM Security Profiles** as you would for any security policy.
6. Select **OK**.

Adding endpoint protection

Optionally, you can require that users’ devices have FortiClient Endpoint Security software installed. FortiOS pushes a FortiClient profile out to the FortiClient software, configuring network protection such as antivirus, application control, and web category filtering. Devices without an up-to-date installation of FortiClient software are restricted to a captive portal from which the user can download a FortiClient installer. For information about creating FortiClient profiles, see "Endpoint Protection".

To add endpoint protection to a security policy

1. Go to **Policy & Objects > Policy > IPv4** and edit the policy.
2. In **Firewall / Network Options** set **Compliant with FortiClient Profile** to **ON**.
   The policy must have device types or gevice groups in the **Source Device Type** field.

Endpoint Protection

This section describes the Endpoint Protection feature and how to configure it.

The following topics are included in this section:

- Endpoint Protection overview
- Configuration overview
- Creating a FortiClient profile
- Enabling Endpoint Protection in security policies
- Configuring endpoint registration over a VPN
- Monitoring endpoints
- Modifying the Endpoint Protection replacement messages

Endpoint Protection overview

Endpoint Protection enforces the use of up-to-date FortiClient Endpoint Security software on endpoints (workstation computers and mobile devices). It pushes a FortiClient profile to the FortiClient application, specifying security settings, including:

- Real-time antivirus protection - on or off
- FortiClient web category filtering based on web filters defined in a FortiGate web filter profile
- FortiClient application control (application firewall) using application sensors defined in the FortiGate application control feature

The FortiClient profile can also specify:

- VPN configurations
- Configuration profile (.mobileconfig file for iOS)
- Dashboard banner

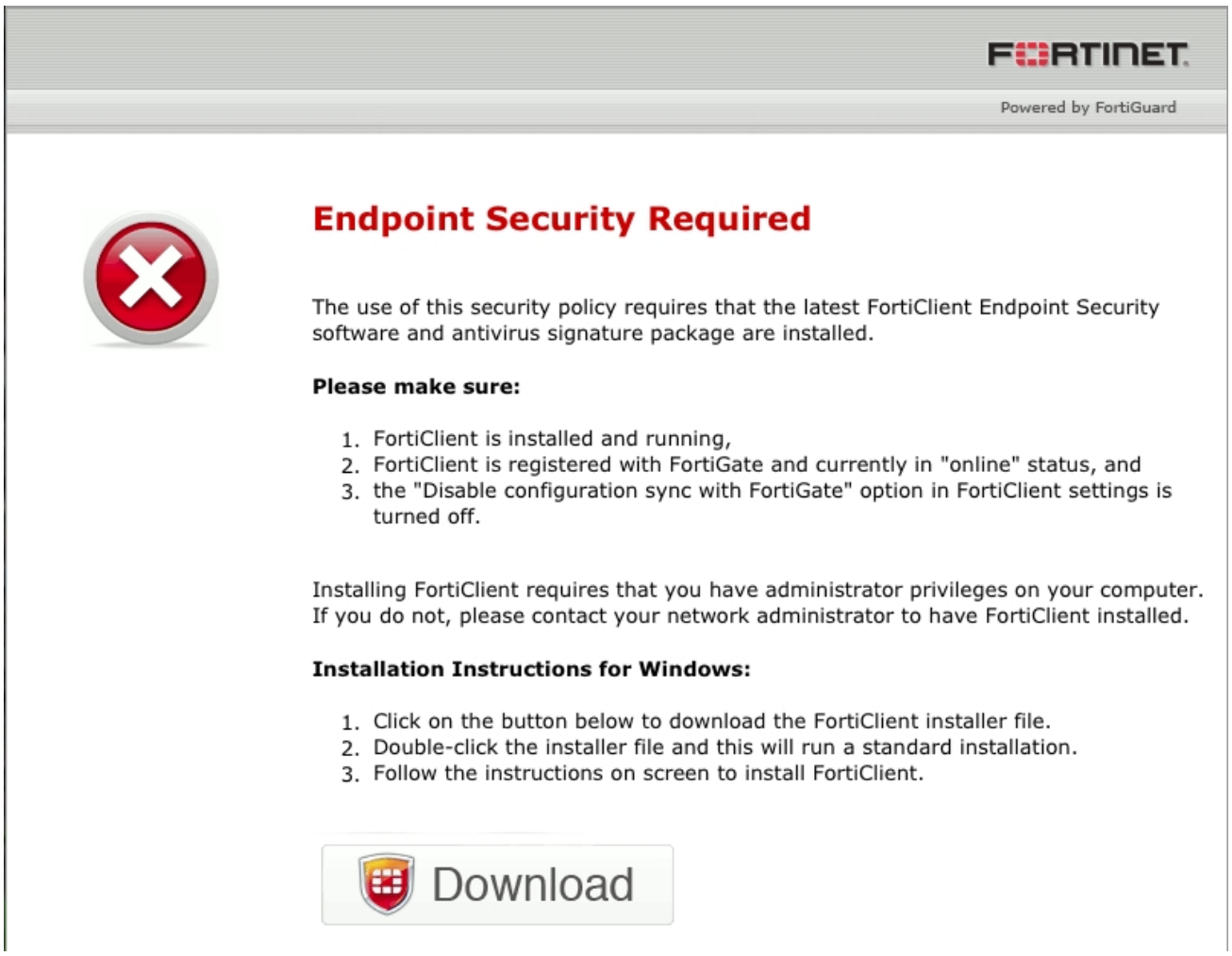
You enable Endpoint Security in security policies by enabling **Compliant with FortiClient Profile**. The policy must specify at least one device type.

User experience

When using a web browser, the user of a non-compliant endpoint receives a replacement message HTML page from the FortiGate unit. The message explains that the user needs to install FortiClient Endpoint Security and provides a link to do so. The user cannot continue until the FortiClient software is installed.

For information about modifying the replacement page, see Modifying the Endpoint Protection replacement messages on page 1958.

Default FortiClient non-compliance message for Windows



After installing FortiClient Endpoint Security, the user will receive an invitation to register with the FortiGate unit. If the user accepts the invitation, the FortiClient profile is sent to the device's FortiClient application. Now the user is compliant with the security policy and can connect to the network. FortiClient Endpoint Security registered with a FortiGate unit does not need to be separately licensed with FortiGuard.

The FortiGate unit can also register endpoints who connect over the Internet through a VPN. The user can accept an invitation to register with the FortiGate unit. See Configuring endpoint registration over a VPN on page 1957.

FortiGate endpoint registration limits

To view the number of endpoints that are registered and the total that can be registered, go to **System > Dashboard > Status**. Under **License Information**, find **FortiClient**. You will see a line like “Registered/Allowed 4 of 10”. This means that there are four registered endpoints and a total of ten are allowed.

When the registration limit is reached, the next FortiClient-compatible device will not be able to register with the FortiGate unit. The user sees a message in FortiClient application about this. The FortiClient profile is not sent to client and the client cannot connect through the FortiGate unit.

For all FortiGate models, the maximum number of registered endpoints is ten. For all models except 20C, you can purchase an endpoint license to increase this capacity:

To add an endpoint license - web-based manager

1. Go to **System > Dashboard > Status**.
2. In the **License Information** widget, under **FortiClient**, select **Enter License**, enter the license key, and select **OK**.

Maximum registered endpoints with endpoint license

Model type	Max Registered Endpoints
30 to 90 series	200
100 to 300 series	600
500 to 800 series, VM1, VM2	2 000
1000 series, VM4	8 000
3000 to 5000 series, VM8	20 000

Configuration overview

Endpoint Protection requires that all hosts using the firewall policy have the FortiClient Endpoint Security application installed. Make sure that all hosts affected by this policy are able to install this application. Currently, FortiClient Endpoint Security is available for Microsoft Windows (2000 and later) and Apple Mac OSX only.

To set up Endpoint Protection, you need to:

- By default, the FortiGuard service provides the FortiClient installer. If you prefer to host it on your own server, see Changing the FortiClient installer download location, below.
- In Security Profiles, configure application sensors and web filter profiles as needed to monitor or block applications. See the Security Profiles Guide for details.
- Create a FortiClient profile or use the default profile. See Creating a FortiClient profile on page 1954. Enable the application sensor and web category filtering profiles that you want to use.
- Enable **Compliant with FortiClient Profile** in the security policies that the endpoints will use.
- Create the registration key for users to register their device with the FortiGate unit.
- Optionally, configure the FortiGate unit to support endpoint registration by IPsec or SSL VPN.
- Optionally, modify the **Endpoint NAC Download Portal** replacement messages (one per platform).

Changing the FortiClient installer download location

By default, FortiClient installers are downloaded from the FortiGuard network. You can also host these installers on a server for your users to download. In that case, you must configure FortiOS with this custom download

location. For example, to set the download location to a customer web server with address custom.example.com, enter the following command:

```
config endpoint-control settings
   set download-location custom
   set download-custom-link "http://custom.example.com"
end
```

Creating a FortiClient profile

There is a default FortiClient profile for Windows and Mac OS that enables only AntiVirus, Web Filtering, and VPN. You can modify this profile or create your own FortiClient profiles.

Except for the default profile, each FortiClient profile is assigned to particular device groups, and optionally to particular users and user groups. If no other FortiClient profile is assigned to a particular device type, the default profile applies. It is possible for more than one profile to be assigned to a device type. As with security policies, clients are matched to FortiClient profiles in the order that the profiles appear in the list.

When **Compliant with FortiClient Profile** is selected in the security policy, all users of that policy must have FortiClient Endpoint Security installed. The FortiGate unit pushes the FortiClient profile settings to the FortiClient application on the client.

To create a FortiClient profile - web-based manager

1. If you will use the Application Firewall feature, go to **Security Profiles > Application Control** to create the Application Sensors that you will need.
2. If you will use Web Category Filtering, go to **Security Profiles > Web Filter** to create the web filter profile that you will need.
3. Go to **User & Device > FortiClient Profiles**.
   If there is only the default FortiClient profile, it is displayed, ready to edit. At the top right of the page you can select or create other profiles.
4. Select **Create New** or select an existing profile and **Edit** it.
5. In **Assign Profile To**, select the device groups, user groups, and users to which this FortiClient profile applies. This is not available for the default profile.
6. Enter the **FortiClient Configuration Deployment** settings for **Windows and Mac**:

Antivirus Protection	ON — enable the FortiClient realtime AntiVirus feature.
Web Category Filtering	ON — enable web category filtering. Select the web filter profile to use.
Client Web Filtering when On-Net	Enable to use FortiClient web filtering.
VPN	ON - enable VPN use by FortiClient.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. Enter the VPN configuration details.
Application Firewall	ON — enable application control. Select the application sensor to use.

Upload Logs to FortiAnalyzer / FortiManager	ON — enable log upload. Specify log device and select schedule.
Use FortiManager for client software/signature update	ON — FortiClient software obtain AV signatures and software updates from the specified FQDN or IP address. **Failover to FDN when FortiManager is not available** is enabled by default.
Dashboard Banner	ON — Display dashboard banner.
Client-based Logging when On-Net	ON — FortiClient will continue to log even when its traffic is flowing through a FortiGate unit.

7. Enter the **FortiClient Configuration Deployment** settings for **iOS**:

Web Category Filtering	ON — enable web category filtering. Select the web filter profile to use.
Client Web Filtering when On-Net	Enable to use FortiClient web filtering.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. You can enter multiple VPN configurations by selecting the “+” button.
VPN Name	Enter a name to identify this VPN configuration in the FortiClient application.
Type	Select **IPsec** or **SSL-VPN**. If you select **IPsec**, select a **VPN Configuration File** that contains the required IPsec VPN configuration. The Apple iPhone Configuration Utility produces .mobileconfig files which contain configuration information for an iOS device. If you select **SSL-VPN**, enter the VPN configuration details.
Distribute Configuration Profile	ON — Distribute configuration information to iOS devices running FortiClient Endpoint Security. Select **Browse** and locate the file to be distributed. The Apple iPhone Configuration Utility produces .mobileconfig files which contain configuration information for an iOS device.

8. Enter the **FortiClient Configuration Deployment** settings for **Android**:

Web Category Filtering	ON — enable web category filtering. Select the web filter profile to use.
Client Filtering when On-Net	Disables FortiClient web category filtering when client traffic is filtered by the FortiGate unit. Selected by default.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. You can enter multiple VPN configurations by selecting the “+” button.

VPN Name	Enter a name to identify this VPN configuration in the FortiClient application.
Type	Select **IPsec** or **SSL-VPN**. Enter the VPN configuration details.

9. Select **OK**.

To create a FortiClient profile - CLI:

This example creates a profile for Windows and Mac computers.

```
config endpoint-control profile
   edit ep-profile1
      set device-groups mac windows-pc
      config forticlient-winmac-settings
         set forticlient-av enable
         set forticlient-wf enable
         set forticlient-wf-profile default
      end
   end
```

Creating the registration key

To register their endpoint devices with the FortiGate unit, users must enter a registration key that you create and provide to them.

To create the FortiClient Endpoint Registration key

1. Go to **System > Config > Advanced**.
2. Enable **FortiClient Endpoint Registration** and enter the key.
   You can create a key containing up to 127 alphanumeric characters.
3. Select **Apply**.

Enabling Endpoint Protection in security policies

Endpoint Protection is applied to any traffic where the controlling firewall policy has Endpoint Security enabled. The device group to which the device belongs determines which FortiClient profile is applied. The policy searches the list of FortiClient profiles starting from the top and applies the first profile assigned to the device group.

To enable Endpoint Protection - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and edit the security policy where you want to enable Endpoint Protection.
   The policy must specify at least one **Source Device Type**.
2. Select **Compliant with FortiClient profile**.
3. Select **OK**.

To configure the firewall policy - CLI:

In this example, the LAN connects to Port 2 and the Internet is connected to Port 1. a FortiClient profile is applied.

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr LANusers
      set dstaddr all
      set devices employee\ laptop
      set schedule always
      set service ALL
      set devices all
      set action accept
      set nat enable
      set endpoint-compliance enable
   end
```

Configuring endpoint registration over a VPN

FortiGate units can register FortiClient-equipped endpoints over either an interface-based IPsec VPN or a tunnel-mode SSL VPN. After the user authenticates, the FortiGate unit sends the FortiClient application the IP address and port to be used for registration. If the user accepts the FortiGate invitation to register, registration proceeds and the FortiClient profile is downloaded to the client.

Users without FortiClient Endpoint Security connecting to the SSL VPN through a browser are redirected to a captive portal to download and install the FortiClient software.

Endpoint registration on an IPsec VPN

You can enable endpoint registration when you configure the FortiClient VPN or you can enable it on an existing FortiClient VPN.

To enable endpoint registration while configuring the VPN

- Enable **Allow Endpoint Registration** on the Policy & Routing page of the VPN Wizard when creating the FortiClient VPN.

To enable endpoint registration on an existing VPN

1. Go to **System > Network > Interfaces** and edit the VPN's tunnel interface.
   The tunnel is a subinterface of the physical network interface.
2. In **Administrative Access**, make sure that **FCT-Access** is enabled.
3. Select **OK**.

Endpoint registration on an SSL VPN

To enable endpoint registration on the SSL VPN

1. Go to **VPN > SSL > Settings.**
2. In **Tunnel Mode Client Settings**, make sure **Allow Endpoint Registration** is enabled.

3. Select **Apply**.

This procedure does not include all settings needed to configure a working SSL VPN.

Synchronizing endpoint registrations

To support roaming users in a network with multiple FortiGate units, you need to configure synchronization of the endpoint registration databases between the units. The registered endpoints are then recognized on all of the FortiGate units. This is configured in the CLI. For example, to synchronize this FortiGate unit's registered endpoint database with another unit named `other1` at IP address 172.20.120.4, enter:

```
config endpoint-control forticlient-registration-sync
   edit other1
      set peer-ip 172.20.120.4
   end
```

Monitoring endpoints

Go to **User & Device > Monitor > FortiClient** to monitor endpoints.

Modifying the Endpoint Protection replacement messages

If the security policy has **Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal** enabled, users of non-compliant devices are redirected to a captive portal that is defined by the **Endpoint NAC Download Portal** replacement message. There are different portals for Android, iOS, Mac, Windows, and "other" devices. Optionally, you can modify them.

To modify the Endpoint NAC Download Portal

1. Go to **System > Config > Replacement Message Group** and select **Extended View**.
2. In the **Endpoint Control** section select the message that you want to edit.
   The replacement message and its HTML code appear in a split screen in the lower half of the page.
3. Modify the text as needed and select **Save**.

Vulnerability Scan

The Network Vulnerability Scan helps you to protect your network assets (servers and workstations) by scanning them for security weaknesses. You can scan on-demand or on a scheduled basis. Results are viewable on the FortiGate unit, but results are also sent to an attached FortiAnalyzer unit. The FortiAnalyzer unit can collect the results of vulnerability scans from multiple FortiGate units at different locations on your network, compiling a comprehensive report about network security.

This section describes how to configure a single FortiGate unit for network scanning and how to view the results of the scan.

The following topics are included in this section:

- Configuring vulnerability scans
- Running a vulnerability scan and viewing scan results
- Requirements for authenticated scanning and ports scanned

Configuring vulnerability scans

You can configure the scan schedule and the assets to be scanned.

To configure scanning - web-based manager:

1. Go to **User & Device > Vulnerability Scan > Scan Definition**.
2. Beside **Schedule** select **Change** to set the scan schedule and mode:

Recurrence	Select **Daily**, **Weekly**, or **Monthly** and configure the details for the option you have selected.
Suspend Scan between	Set a time during which the scan should be paused if its running. (Optional)
Vulnerability Scan Mode	**Quick** — check only the most commonly used ports **Standard** — check the ports used by most known applications **Full** — check all TCP and UDP ports For a detailed list of the TCP and UDP ports examined by each scan mode, see Ports scanned in each scan mode on page 1964.

3. Select **Apply** to save the configuration.
4. In **Asset Definitions**, click Create New and enter information about the asset:

Name	Enter a name for this asset.
Type	Select **IP Address** to add a single IP address. Select **Range** to add a range of IP addresses to scan.
IP Address	Enter the IP address of the asset. (**Type** is **IP Address**.)
Range	Enter the start and end of the IP address range. (**Type** is **Range**.)
Enable Scheduled Vulnerability Scanning	Select to allow this asset to be scanned according to the schedule. Otherwise the asset is not scanned during a scheduled vulnerability scan.
Windows Authentication	Select to use authentication on a Windows operating system. Enter the username and password in the fields provided. For more information, see Requirements for authenticated scanning and ports scanned on page 1961.
Unix Authentication	Select to use authentication on a Unix operating system. Enter the username and password in the fields provided. For more information, see Requirements for authenticated scanning and ports scanned on page 1961.

To configure scanning - CLI:

To configure, for example, a standard scan to be performed every Sunday at 2:00am, you would enter:

```
config netscan settings
   set scan-mode standard
   set schedule enable
   set time 02:00
   set recurrence weekly
   set day-of-week sunday
end
```

To add an asset - CLI:

This example adds a single computer to the Asset list:

```
config netscan assets
   edit 0
      set name "server1"
      set addr-type ip
      set start-ip 10.11.101.20
      set auth-windows enable
      set win-username admin
      set win-password zxcvbnm
      set scheduled enable
   end
```

This example adds an address range to the Asset list. Authentication is not used:

```
config netscan assets
   edit 0
      set name "fileservers"
      set addr-type range
      set start-ip 10.11.101.160
      set end-ip 10.11.101.170
```

```
    set scheduled enable
end
```

Running a vulnerability scan and viewing scan results

To run a vulnerability scan - web-based manager:

1. Go to **User & Device > Vulnerability Scan > Scan Definition** and select **Start Scan**.
   When the scan is running you can pause or stop it at any time. You can also watch the progress of the scan.
2. When the scan is complete go to **User & Device > Vulnerability Scan > Vulnerability Result** to view the results of the scan.

To run a vulnerability scan - CLI:

Use the following CLI commands:

```
execute netscan start scan
execute netscan status
execute netscan pause
execute netscan resume
execute netscan stop
```

To view vulnerability scan results:

- To view vulnerability scan results go to **User & Device > Vulnerability Scan > Vulnerability Result**.

Select any log entry to view log details.

Requirements for authenticated scanning and ports scanned

The effectiveness of an authenticated scan is determined by the level of access the FortiGate unit obtains to the host operating system. Rather than use the system administrator's account, it might be more convenient to set up a separate account for the exclusive use of the vulnerability scanner with a password that does not change.

The following sections detail the account requirements for various operating systems.

Microsoft Windows hosts - domain scanning

The user account provided for authentication must

- have administrator rights
- be a Security type of account
- have global scope
- belong to the Domain Administrators group
- meet the Group Policy requirements listed below:

Group Policy - Security Options

In the Group Policy Management Editor, go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.

Setting	Value
Network access: Sharing and security model for local accounts	Classic
Accounts: Guest account status	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Group Policy - System Services

In the Group Policy Management Editor, go to **Computer Configuration > Windows Settings > Security Settings > System Services**.

Setting	Value
Remote registry	Automatic
Server	Automatic
Windows Firewall	Automatic

Group Policy - Administrative Templates

In the Group Policy Management Editor, go to **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.

Setting	Value
Windows Firewall: Protect all network connections	Disabled

or

Setting	Value
Windows Firewall: Protect all network connections	Enabled
Windows Firewall: Allow remote administration exception	Enabled
Allow unsolicited messages from[1]	*
Windows Firewall: Allow file and printer sharing exception	Enabled
Allow unsolicited messages from[1]	*
Windows Firewall: Allow ICMP exceptions	Enabled
Allow unsolicited messages from[1]	*

[1]Windows prompts you for a range of IP addresses. Enter either "*" or the IP address of the Fortinet appliance that is performing the vulnerability scan.

Microsoft Windows hosts - local (non-domain) scanning

The user account provided for authentication must:

- be a local account
- belong to the Administrators group

The host must also meet the following requirements:

- Server service must be enabled. (Windows 2000, 2003, XP)
- Remote Registry Service must be enabled.
- File Sharing must be enabled.
- Public folder sharing must be disabled. (Windows 7)
- Simple File Sharing (SFS) must be disabled. (Windows XP)

Windows firewall settings

Enable the **Remote Administration Exception** in Windows Firewall. (Windows 2003, Windows XP)

Allow **File and Print sharing** and **Remote Administration** traffic to pass through the firewall. Specify the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows Vista, 2008)

For each of the active **Inbound Rules** in the **File and Printer Sharing** group, set the **Remote IP address** under **Scope** to either **Any IP address** or to the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows 7)

Unix hosts

The user account provided for authentication must be able at a minimum to execute these commands:

- The account must be able to execute "uname" in order to detect the platform for packages.
- If the target is running Red Hat, the account must be able to read /etc/redhat-release and execute "rpm".
- If the target is running Debian, the account must be able to read /etc/debian-version and execute "dpkg".

Ports scanned in each scan mode

Scan Type	Ports scanned
Standard Scan	**TCP:** 1-3, 5, 7, 9, 11, 13, 15, 17-25, 27, 29, 31, 33, 35, 37-39, 41-223, 242-246, 256-265, 280-282, 309, 311, 318, 322-325, 344-351, 363, 369-581, 587, 592-593, 598, 600, 606-620, 624, 627, 631, 633-637, 666-674, 700, 704-705, 707, 709-711, 729-731, 740-742, 744, 747-754, 758-765, 767, 769-777, 780-783, 786, 799-801, 860, 873, 886-888, 900-901, 911, 950, 954-955, 990-993, 995-1001, 1008, 1010-1011, 1015, 1023-1100, 1109-1112, 1114, 1123, 1155, 1167, 1170, 1207, 1212, 1214, 1220-1222, 1234-1236, 1241, 1243, 1245, 1248, 1269, 131t3-1314, 1337, 1344-1625, 1636-1774, 1776-1815, 1818-1824, 1901-1909, 1911-1920, 1944-1951, 1973, 1981, 1985-2028, 2030, 2032-2036, 2038, 2040-2049, 2053, 2065, 2067, 2080, 2097, 2100, 2102-2107, 2109, 2111, 2115, 2120, 2140, 2160-2161, 2201-2202, 2213, 2221-2223, 2232-2239, 2241, 2260, 2279-2288, 2297, 2301, 2307, 2334, 2339, 2345, 2381, 2389, 2391, 2393-2394, 2399, 2401, 2433, 2447, 2500-2501, 2532, 2544, 2564-2565, 2583, 2592, 2600-2605, 2626-2627, 2638-2639, 2690, 2700, 2716, 2766, 2784-2789, 2801, 2908-2912, 2953-2954, 2998, 3000-3002, 3006-3007, 3010-3011, 3020, 3047-3049, 3080, 3127-3128, 3141-3145, 3180-3181, 3205, 3232, 3260, 3264, 3267-3269, 3279, 3306, 3322-3325, 3333, 3340, 3351-3352, 3355,

Scan Type	Ports scanned
Standard Scan	**TCP Continued**: 3372, 3389, 3421, 3454-3457, 3689-3690, 3700, 3791, 3900, 3984-3986, 4000-4002, 4008-4009, 4080, 4092, 4100, 4103, 4105, 4107, 4132-4134, 4144, 4242, 4321, 4333, 4343, 4443-4454, 4500-4501, 4567, 4590, 4626, 4651, 4660-4663, 4672, 4899, 4903, 4950, 5000-5005, 5009-5011, 5020-5021, 5031, 5050, 5053, 5080, 5100-5101, 5145, 5150, 5190-5193, 5222, 5236, 5300-5305, 5321, 5400-5402, 5432, 5510, 5520-5521, 5530, 5540, 5550, 5554-5558, 5569, 5599-5601, 5631-5632, 5634, 5678-5679, 5713-5717, 5729, 5742, 5745, 5755, 5757, 5766-5767, 5800-5802, 5900-5902, 5977-5979, 5997-6053, 6080, 6103, 6110-6112, 6123, 6129, 6141-6149, 6253, 6346, 6387, 6389, 6400, 6455-6456, 6499-6500, 6515, 6558, 6588, 6660-6670, 6672-6673, 6699, 6767, 6771, 6776, 6831, 6883, 6912, 6939, 6969-6970, 7000-7021, 7070, 7080, 7099-7100, 7121, 7161, 7174, 7200-7201, 7300-7301, 7306-7308, 7395, 7426-7431, 7491, 7511, 7777-7778, 7781, 7789, 7895, 7938, 7999-8020, 8023, 8032, 8039, 8080-8082, 8090, 8100, 8181, 8192, 8200, 8383, 8403, 8443, 8450, 8484, 8732, 8765, 8886-8894, 8910, 9000-9001, 9005, 9043, 9080, 9090, 9098-9100, 9400, 9443, 9535, 9872-9876, 9878, 9889, 9989-10000, 10005, 10007, 10080-10082, 10101, 10520, 10607, 10666, 11000, 11004, 11223, 12076, 12223, 12345-12346, 12361-12362, 12456, 12468-12469, 12631, 12701, 12753, 13000, 13333, 14237-14238, 15858, 16384, 16660, 16959, 16969, 17007, 17300, 18000, 18181-18186, 18190-18192, 18194, 18209-18210, 18231-18232, 18264, 19541, 20000-20001, 20011, 20034, 20200, 20203, 20331, 21544, 21554, 21845-21849, 22222, 22273, 22289, 22305, 22321, 22555, 22800, 22951, 23456, 23476-23477, 25000-25009, 25252, 25793, 25867, 26000, 26208, 26274, 27000-27009, 27374, 27665, 29369, 29891, 30029, 30100-30102, 30129, 30303, 30999, 31336-31337, 31339, 31554, 31666, 31785, 31787-31788, 32000, 32768-32790, 33333, 33567-33568, 33911, 34324, 37651, 40412, 40421-40423, 42424, 44337, 47557, 47806, 47808, 49400, 50505, 50766, 51102, 51107, 51112, 53001, 54321, 57341, 60008, 61439, 61466, 65000, 65301, 65512 **UDP:** 7, 9, 13, 17, 19, 21, 37, 53, 67-69, 98, 111, 121, 123, 135, 137-138, 161, 177, 371, 389, 407, 445, 456, 464, 500, 512, 514, 517-518, 520, 555, 635, 666, 858, 1001, 1010-1011, 1015, 1024-1049, 1051-1055, 1170, 1243, 1245, 1434, 1492, 1600, 1604, 1645, 1701, 1807, 1812, 1900, 1978, 1981, 1999, 2001-2002, 2023, 2049, 2115, 2140, 2801, 3024, 3129, 3150, 3283, 3527, 3700, 3801, 4000, 4092, 4156, 4569, 4590, 4781, 5000-5001, 5036, 5060, 5321, 5400-5402, 5503, 5569, 5632, 5742, 6073, 6502, 6670, 6771, 6912, 6969, 7000, 7300-7301, 7306-7308, 7778, 7789, 7938, 9872-9875, 9989, 10067, 10167, 11000, 11223, 12223, 12345-12346, 12361-12362, 15253, 15345, 16969, 20001, 20034, 21544, 22222, 23456, 26274, 27444, 30029, 31335, 31337-31339, 31666, 31785, 31789, 31791-31792, 32771, 33333, 34324, 40412, 40421-40423, 40426, 47262, 50505, 50766, 51100-51101, 51109, 53001, 61466, 65000
Full Scan	All TCP and UDP ports (1-65535)

Scan Type	Ports scanned
Quick Scan	**TCP:** 11, 13, 15, 17, 19-23, 25, 37, 42, 53, 66, 69-70, 79-81, 88, 98, 109-111, 113, 118-119, 123, 135, 139, 143, 220, 256-259, 264, 371, 389, 411, 443, 445, 464-465, 512-515, 523-524, 540, 548, 554, 563, 580, 593, 636, 749-751, 873, 900-901, 990, 992-993, 995, 1080, 1114, 1214, 1234, 1352, 1433, 1494, 1508, 1521, 1720, 1723, 1755, 1801, 2000-2001, 2003, 2049, 2301, 2401, 2447, 2690, 2766, 3128, 3268-3269, 3306, 3372, 3389, 4100, 4443-4444, 4661-4662, 5000, 5432, 5555-5556, 5631-5632, 5634, 5800-5802, 5900-5901, 6000, 6112, 6346, 6387, 6666-6667, 6699, 7007, 7100, 7161, 7777-7778, 8000-8001, 8010, 8080-8081, 8100, 8888, 8910, 9100, 10000, 12345-12346, 20034, 21554, 32000, 32768-32790 **UDP:** 7, 13, 17, 19, 37, 53, 67-69, 111, 123, 135, 137, 161, 177, 407, 464, 500, 517-518, 520, 1434, 1645, 1701, 1812, 2049, 3527, 4569, 4665, 5036, 5060, 5632, 6502, 7778, 15345

Chapter 20 - Managing a FortiSwitch with a FortiGate

Managing a FortiSwitch with a FortiGate

Introduction

This document describes how to use FortiGate to remotely manage FortiSwitch units, which is also known as using a FortiSwitch in FortiLink mode. FortiLink defines the management interface and the remote management protocol between the FortiGate and FortiSwitch.

FortiGate supports remote management for up to 16 FortiSwitches.

Supported Models

The following table shows the FortiSwitch models that support FortiLink mode when paired with the corresponding FortiGate models and the listed minimum software releases.

FortiSwitch	FortiGate	Earliest FortiSwitchOS	Earliest FortiOS
FS-224D-POE	FGT-90D(Wifi/poe) + FGT-Models1	3.0.0	5.2.2
FS-108D-POE	FGT-60D(all) + FGT-Models1	3.0.1	5.2.3
FSR-112D-POE	FGR-90D + FGT-Models1	3.0.1	5.2.3
FS-124D	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3
FS-124D-POE	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3
FS-224D-FPOE	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3

FortiGate models 1 includes the following: 100D/200D/240D/140D(POE, T1),280D(POE)/600C/800C/1000C

Before You Begin

Before you set up remote management of your FortiSwitch unit, certain assumptions have been made in the writing of this manual:

- You have installed a FortiGate unit on your network and have administrative access to the FortiGate web-based manager and CLI.

How this Guide is Organized

This guide contains the following sections:

Getting Started - describes how to configure the FortiGate for remote management of the FortiSwitch units.

VLAN Configuration - configure VLANs from the FortiGate unit.

Port Configuration - configure Ports from the FortiGate unit.

Scenarios - contains practical examples of how to use the FortiGate unit to manage a network of FortiSwitches.

Getting Started

This chapter describes how to configure the FortiGate to provide remote management for FortiSwitch units.

The FortiGate requires a one-time configuration task to enable the Switch Controller on the FortiGate.

Adding a new managed FortiSwitch is very simple. You connect a cable from a port on the FortiGate to the designated FortiLink port on the FortiSwitch. Using the FortiGate GUI, you then set two simple configuration settings. No configuration changes are required on the FortiSwitch (one change is required in FortiSwitchOS releases prior to 3.3.0).

Optionally, you can also configure remote management access directly to the FortiSwitch.

Enable the Switch Controller on FortiGate

Prior to configuring the first managed FortiSwitch, you must enable the Switch Controller on the FortiGate unit. If the main left menu already contains the **WiFi & Switch Controller** entry, you can skip this step.

Using the FortiGate web-based manager

1. Go to **System > Config > Features**.
2. Set the **WiFi & Switch Controller** feature to **on**.
3. Select **Apply**.

The menu now includes the **WiFi & Switch Controller** entry.

Using the FortiGate CLI

Use the following command to enable the Switch Controller and set the reserved subnetwork for the controller:

```
config system global
   set switch-controller enable
   set switch-controller-reserved-network 169.254.254.0 255.255.255.0
end
```

Adding a Managed FortiSwitch with FortiGate GUI

The procedure to add a new managed FortiSwitch consists of the following simple steps using the FortiGate GUI:

Note: For FortiSwitchOS releases prior to 3.3.0, you must Set the FortiSwitch to remote management mode prior to starting step 1

1. Connect a cable from the designated FortiSwitch port to an unused port on the FortiGate. For example, use port 24 on the FS-224D-POE switch. Refer to FortiLink Port for each FortiSwitch Model for additional information.
2. Go to **System > Network > Interfaces** and edit an internal port on the FortiGate.
3. Set **Addressing mode** to **Dedicate to Extension Device**.
4. Select **OK**.
5. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiSwitch**.
   The new FortiSwitch should now be displayed in the table.
6. Right-click on the FortiSwitch and select **Authorize**.

After a delay (while FortiGate processes the request), an icon with a green checkmark appears in the Status column. For smaller FortiSwitch models, such as FS-108D-POE, the delay may be up to 3 minutes.

Set the FortiSwitch to remote management mode

Use the FortiSwitch web-based manager or the CLI to set remote management mode.

Note: This configuration step is not required in FortiSwitchOS release 3.3.0 or later releases.

Using the FortiSwitch web-based manager

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Beside **Operation Mode**, select **Change**.
3. Change **Management Mode** to **FortiGate Remote Management**.
4. Select **OK**.
5. A warning will appear, asking if you wish to continue. Select **OK**.

Using the FortiSwitch CLI

Use the following command to change the FortiSwitch management mode:

```
config system global
   set switch-mgmt-mode fortilink
end
```

The FortiSwitch unit is now ready to be connected to the FortiGate unit.

FortiLink Port for each FortiSwitch Model

Each FortiSwitch model provides one designated port for the FortiLink connection. The table below lists the FortiLink port for each model:

FortiSwitch Model	Port for FortiLink connection
FS-28C	WAN port 1
FS-324B-POE	Management Port
FS-448B (10G only)	WAN port (uplink 1)
FS-348B	Last port (port 48)
For all D-series switches, use the last (highest number) port for FortiLink. For example:	
FS-108D-POE	Last port (port 10)
FSR-112D-POE	Last port (port 12)
FS-124D	Last port (port 26). May require an SFP module. See note below the table.
FS-224D-POE	Last port (port 24)
FS-224D-FPOE	Last port (port 28). May require an SFP module. See note below the table.

Note: FortiSwitch 3.3.1 and later releases support the use of an RJ-45 port for FortiLink.
Please contact Fortinet Customer Support for additional information.

FortiLink Ports for Each FortiGate Model

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit.

The following table shows the ports for each model of FortiGate that can be FortiLink-dedicated.

FortiGate Model	Ports for FortiLink connection
FGT-90D, FGT-90D-POE FWF-90D, FWF-90D-POE	port1 - port14
FGT-60D, FGT-60D-POE FWF-60D, FWF-60D-POE	port1 - port7
FGT-100D	port1 - port16
FGT-140D , 140D-POE, 140D-POE-T1	port1 - port36
FGT-200D	port1 - port16
FGT-240D	port1 - port40
FGT-280D, FGT-280D-POE	port1 - port84
FGT-600C	port3 - port22
FGT-800C	port3 - port24
FGT-1000C	port3 - port14, port23 - port24

Adding a Managed FortiSwitch with FortiGate CLI

We recommend that you add a new managed FortiSwitch using the FortiGate GUI. However, the following steps show how to add a new managed FortiSwitch using the FortiGate CLI. In these steps, the FortiGate port1 is configured as the FortiLink port:

1. If required, remove port 1 from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port1
      end
   end
end
```

2. Configure the interface for port 1.

```
config system interface
   edit port1
      set ip 172.20.120.10 255.255.255.0
      set allowaccess capwap
      set vlanforward enable
   end
end
```

3. Configure an NTP server on port 1.

```
config system ntp
   set server-mode enable
   set interface port1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
NOTE: FortiSwitch will reboot when you issue the above command.
```

5. Configure a DHCP server on port 1.

```
config system dhcp server
   edit 0
      set netmask 255.255.255.252
      set interface port1
      config ip-range
         edit 0
            set start-ip 169.254.254.2
            set end-ip 169.254.254.50
         end
      set vci-match enable
      set vci-string FortiSwitch
      set ntp-service local
   end
end
```

Configuring FortiSwitch Remote Management Port

If the FortiSwitch model has a dedicated management port, you can configure remote management to the FortiSwitch. In FortiLink mode, the FortiGate is the default gateway, so you need to configure an explicit route for the FortiSwitch management port.

From the FortiSwitch CLI, enter the following commands:

```
config router static
   edit 1
      set device mgmt
      set gateway <router IP address>
      set dst <router subnet> <subnet mask>
   end
end
```

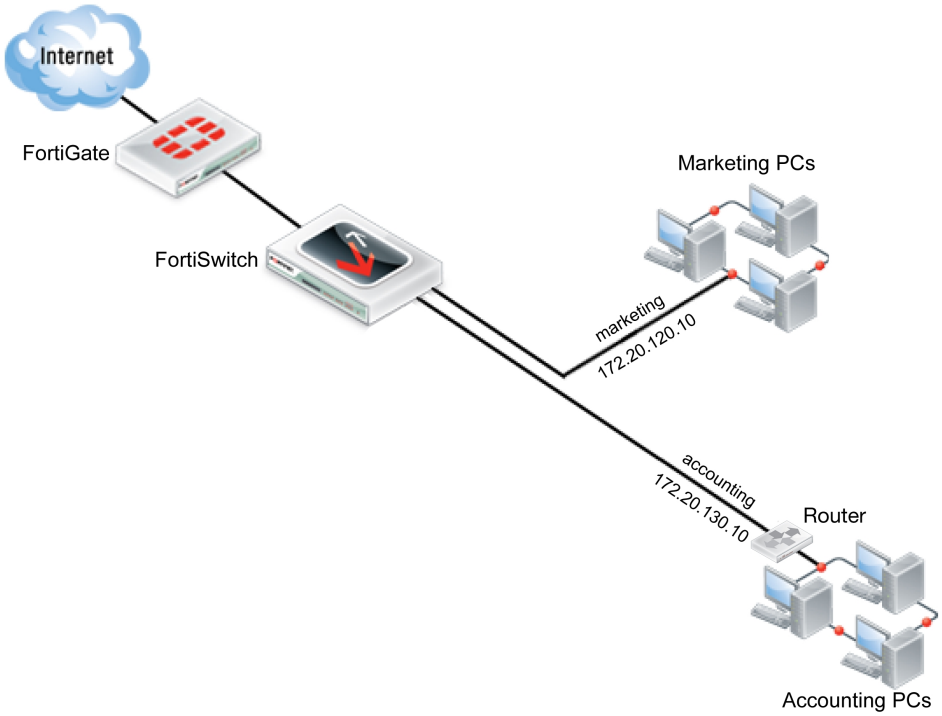
In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
      set dst 192.168.0.0 255.255.0.0
   end
end
```

VLAN Configuration

Using Virtual Local Area Networks (VLANs) allows you to get the most out of using your FortiSwitch unit by using ID tags to logically separate a LAN into smaller broadcast domains. A single LAN can contain many unique VLANs, which allows different policies to be created for different types of users and segments traffic so that it is only sent to and from the intended VLAN.

For example, if a company has one LAN which is to be used for both the marketing and the accounting department, this LAN can be segmented into two VLANs. This allows the traffic from each department to be isolated, so information packets sent to the marketing department are only sent on the marketing VLAN. It also allowed different policies to be created, so that security can be increased for the accounting department without also increasing it for the marketing department.



Now that your FortiSwitch unit is managed by your FortiGate unit, a VLAN can be configured on the FortiSwitch, using the FortiGate.

The following instructions will create a VLAN to be used by the marketing team for network and Internet access. The PCs used by the marketing team will connect to ports 3-6 on the FortiSwitch unit.

Setting up a VLAN requires:

- Creating the VLAN.
- Assigning ports on the FortiSwitch unit to the VLAN.

Creating VLANs

Using the web-based manager

Creating the VLAN

1. Go to **WiFi & Switch Controller** > **Switch Network** > **Virtual Switch** and select **Create New**. Change the following settings:

Name	marketing
Color	
IP/Network Mask	172.20.120.10/255.255.255.0

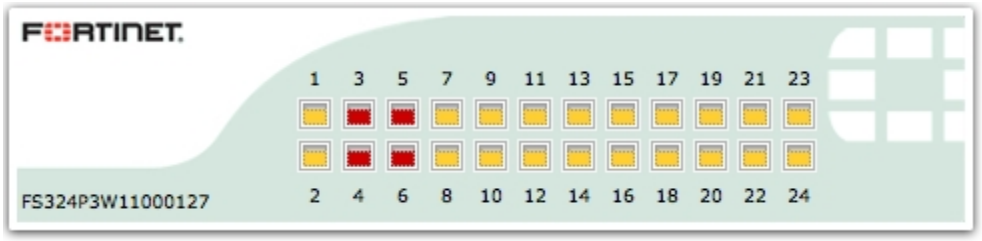
1. Enable **DHCP Server.** Set the IP range to 172.20.120.11-172.20.120.254.
2. Select **OK**.

The entry **marketing** is now shown on the list of **Virtual Switches**. A **marketing** interface has also been added, which can be seen by going to **System > Network > Interfaces**.

Assigning FortiSwitch Ports to the VLAN

1. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch**
2. Highlight the FortiSwitch unit and select **Edit Managed FortiSwitch**.
3. Click and drag a box around ports 3-6 to select them.
4. Select **marketing** from the **Assign to** list.

Ports 3-6 on the FortiSwitch have now been assigned to the marketing VLAN and will appear in red.



Using the CLI

1. Create the marketing VLAN.

```
config switch-controller vlan
   edit marketing
      set color 32
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.120.14 255.255.255.0
end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway 172.20.120.10
      set dns-service default
      set interface marketing
         config ip-range
            set start-ip 172.20.120.11
            set end-ip 172.20.120.254
         end
      set netmask 255.255.255.0
end
```

4. Assign ports 3-6 to the VLAN.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port3
            set vlan marketing
         next
         edit port4
            set vlan marketing
         next
         edit port5
            set vlan marketing
         next
         edit port6
            set vlan marketing
      end
end
```

Setting up a security policy for the VLAN

The following instructions configure a basic security policy for the marketing VLAN that will allow all traffic from the marketing VLAN to have access to the Internet.

Using the web-based manager

1. Go to **Policy & Objects** > **Policy > IPv4** and select **Create New**. Change the following settings:

Incoming Interface	marketing
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Enable NAT	Enable
Logging Options	Log all Sessions

2. Select **OK**.

With this security policy in place, all computers connected to the marketing VLAN can now access the Internet.

Using the CLI

Create a security policy for the marketing VLAN.

```
config security policy
   edit 2
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set logtraffic all
      set nat enable
end
```

Port Configuration

You can configure the FortiSwitch port and POE settings from the FortiGate using CLI commands. Currently, these functions are not available in the FortiGate web-based manager.

The following port CLI commands are available:

- Set port speed.
- Set port admin status
- Configure vlan on the port

Port CLI commands

```
config switch-controller
   edit <switch>
      config ports
         edit <port>
            speed <speed>
            status {down | up}
            vlan <vlan_id>
```

Scenarios

This chapter contains practical examples of how to use the FortiSwitch unit to manage a network. The scenarios are as follows:

- Scenario 1: Allowing access to specific users on the marketing VLAN
- Scenario 2: Adding a specific device to the marketing VLAN
- Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN
- Scenario 4: Configuring the accounting VLAN using an SFP port
- Scenario 5: Connecting a VoIP phone to the FortiSwitch
- Scenario 6: Connecting a FortiAP unit to the FortiSwitch

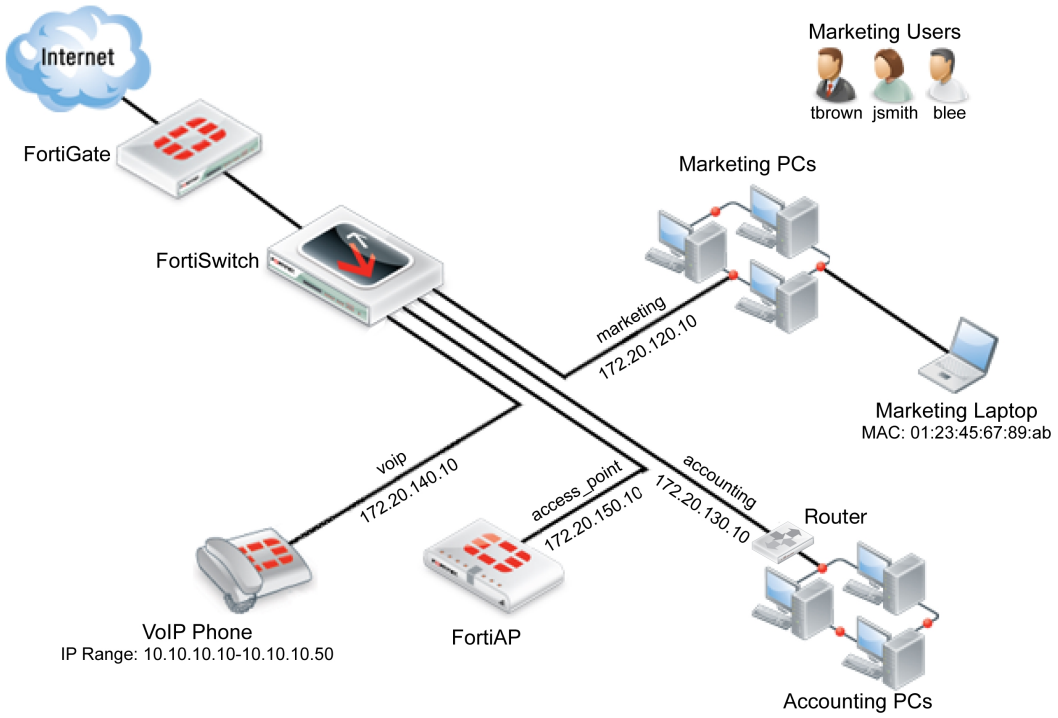
The Example Network

All the scenarios are interrelated and are used to manage an example network with the following attributes:

- The FortiSwitch unit used is a FortiSwitch-224D-POE, serial number FS224D3W14000370.
- The FortiSwitch unit's port 24 connects to port1 on the FortiGate unit.
- The LAN is divided into four distinct VLANs, configured as follows:

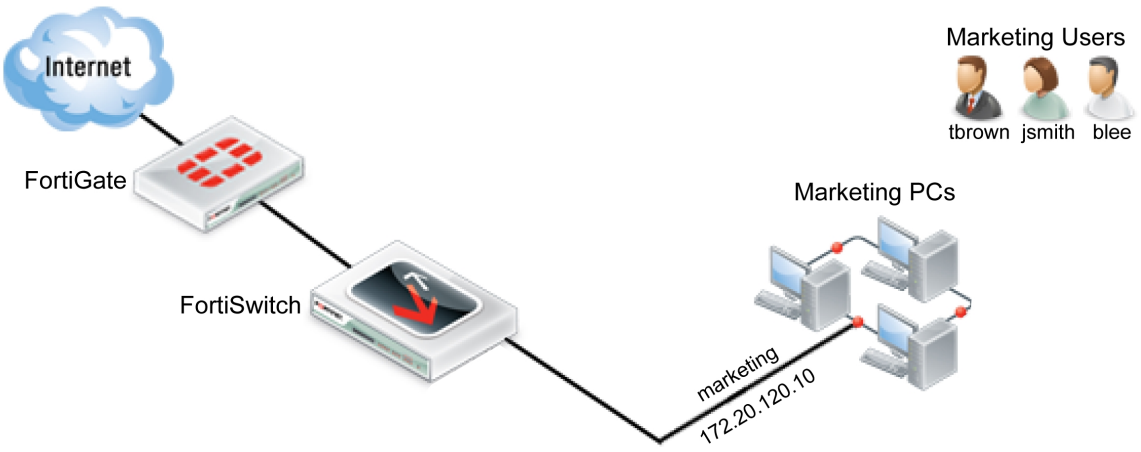
VLAN	IP	Device(s)	Port(s)	Policy ID(s)	GUI Color
marketing	172.20.120.10/255.255.255.0	marketing PCs, marketing laptop	3-6	2, 3	
accounting	172.20.130.10/255.255.255.0	accounting PCs	21	4	
voip	172.20.140.10/255.255.255.0	VoIP phone	10	5	
access_point	172.20.150.10/255.255.255.0	FortiAP	1	6	

- There are six devices that connect directly to the FortiSwitch unit's ports using Ethernet cables: the 3 marketing PCs, the marketing laptop, the VoIP phone, and the FortiAP unit.
- The accounting VLAN connects to the FortiSwitch using an SFP port.
- There are three marketing employees (Jane Smith, Tom Brown, Bob Lee) who will use the marketing VLAN using the marketing PCs.
- The MAC address of the marketing laptop is 01:23:45:67:89:ab.
- The IP range for the VoIP phone is 10.10.10.10-10.10.10.50.
- The FortiAP unit is a FortiAP-11C, serial number FAP11C3X12000412.



Scenario 1: Allowing access to specific users on the marketing VLAN

In Scenario 1, the policies for the marketing VLAN will be created so that different users have different access. The firewall policy will be created so that all three marketing employees (Jane Smith, Tom Brown, Bob Lee) have user accounts. These accounts will be put into one of two groups: full-time and part-time. Full-time employees will always have network access, while part-time employees will only have access on Mondays, Wednesdays and Fridays. This policy will apply to each user when they use any of the PCs that connect to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch.



Creating a policy to match scenario 1 requires:

- Creating users.
- Creating groups.
- Creating a schedule.
- Configuring the firewall policies.

Using the web-based manager

Creating a User Group

1. Go to **User & Device** > **User** > **User Groups** and select **Create New**.
2. Name the user group **part-time**.
3. Set **Type** as **Firewall**.
4. Select **OK**.

The entry **part-time** will now appear on the user group list. Repeat these steps to create another user group, named **full-time**.

Creating a User

1. Go to **User & Device** > **User** > **User Definition**. Select **Create New**.
2. Use the **User Creation Wizard** to create a user. In part 1, select **Local User**.
3. In part 2, change the following settings:

User Name	blee
Password	password

4. In part 3, enter the email address blee@example.com
5. In part 4, select **Enable** and **User Group**. Set **part-time** as the group.
6. Select **Done**.

The entry **blee** will now appear in the user list. Repeat these steps to create user accounts **tbrown** and **jsmith** and add both of these accounts to the **full-time group.**

Creating a Schedule

1. Go to **Policy & Objects** > **Objects** > **Schedules**. Select **Create New** and then select **Recurring**.
2. Change the following settings:

Name	part-time_schedule
Day of the Week	Monday, Wednesday, Friday

3. Select **OK**.

The entry **part-time schedule** will now appear on the schedules list.

Configuring the Firewall Policy

1. Go to **Policy & Objects** > **Policy** > **IPv4** and select **Create New**.
2. Set the policy to use the following the following settings, allowing access for part-time employees:

Incoming Interface	marketing
Source Address	all
Source User(s)	part-time
Outgoing Interface	wan1
Destination Address	all
Schedule	part-time_schedule
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **Policy & Objects** > **Policy> IPv4** and create a new policy.
5. Change the following settings to set access for full-time employees:

Incoming Interface	marketing
Source Address	all
Source User(s)	full-time
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Logging Options	Log all Sessions

6. Select **OK**.

You have now finished creating the policies that match scenario 1. These policies will apply to all three users when they use any of the PCs that connect to the marketing VLAN.

Using the CLI

1. Create the 3 users.

```
config user local
   edit blee
      set type password
      set passwd password
```

```
   next
   edit tbrown
      set type password
      set passwd password
   next
   edit jsmith
      set type password
      set passwd password
end
```

2. Create the 2 user groups and add the users to them.

```
config user group
   edit part-time
      set group-type firewall
      set member blee
next
   edit full-time
      set group-type firewall
      set member tbrown jsmith
end
```

3. Create the schedule for part-time employees.

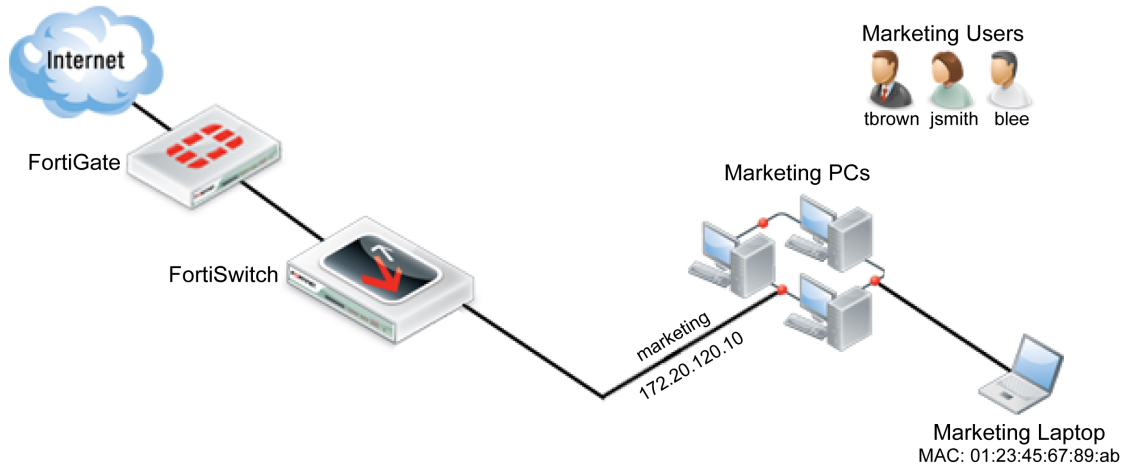
```
config firewall schedule recurring
   edit part-time_schedule
      set day monday wednesday friday
end
```

4. Create two firewall policies for the marketing VLAN, one for each user group:

```
config firewall policy
   edit 2
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set nat enable
      set action accept
      set schedule part-time_schedule
      set logtraffic all
      set groups part-time
      set service ALL
   next
   edit 3
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set nat enable
      set action accept
      set schedule always
      set logtraffic all
      set groups full-time
      set service ALL
end
```

Scenario 2: Adding a specific device to the marketing VLAN

In Scenario 2, a new policy will be created for the marketing VLAN that will be used by the marketing laptop. This policy will affect the marketing laptop that is used periodically for tasks such as boardroom presentations or for guests, tasks for which the laptop requires Internet access. The laptop will access the Internet by connecting to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch. Adding a new policy for the laptop will allow it to connect without requiring user authentication and will also limit the scope of the device's access.



Creating a policy to match scenario 2 requires:

- Assigning a reserve IP to the laptop.
- Creating a firewall address for the reserve IP.
- Creating a firewall policy that uses the reserve IP.

Using the web-based manager

Assigning a Reserve IP to the Laptop

1. Go to **System > Network > Interfaces** and select **marketing**.
2. Under **DHCP Server**, expand the **Advanced** options.
3. In the **MAC Address Access Control List** and select **Create New**.
4. Change the following settings:

MAC	01:23:45:67:89:ab
IP	172.20.120.254
Action	Reserve IP

Creating a Firewall Address for the Reserve IP

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Change the following settings:

Category	Address
Name	marketing_laptop
Type	Subnet
Subnet/IP Range	172.20.120.254
Interface	marketing

Configuring a Firewall Policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Change the following settings:

Incoming Interface	marketing
Source Address	marketing_laptop
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK.**
4. In the policy list, select the column on the far left for the new policy (usually **Seq #)** and drag the policy above the previous policy for the marketing VLAN. This will ensure that the laptop will be identified through this policy.

You have now finished creating a policy that matches scenario 2. This policy will apply to anyone who uses the laptop to connect to the **marketing** VLAN using an Ethernet cable.

Using the CLI

1. Assign a reserve IP to the laptop.

```
config system dhcp server
   edit 2
      config reserved-address
         edit 1
            set action reserved
            set ip 172.20.120.254
            set mac 01:23:45:67:89:ab
      end
end
```

2. Create a firewall address for the reserve IP.

```
config firewall address
```

```
   edit marketing_laptop
      set subnet 172.20.120.254
end
```

3. Create a firewall policy for the marketing VLAN that uses the reserve IP.

```
config firewall policy
   edit 4
      set srcintf marketing
      set dstintf wan1
      set srcaddr marketing_laptop
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP HTTPS DNS
      set logtraffic all
      set nat enable
end
```

4. Place the new firewall policy at the top of the policy list.

```
config firewall policy
   move 4 before 2
end
```

Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN

In Scenario 3, a policy is created to allow remote access to the marketing VLAN, using a virtual private network (VPN) tunnel. This policy will allow marketing employee Tom Brown to connect to the marketing VLAN remotely from his home. The default IP Pool, **SSLVPN_TUNNEL_ADDR1**, will be used to configure the SSL VPN web portal. The computer Tom Brown is using to access the network remotely has a dynamic IP address and will be using the FortiClient application to auto connect to the VPN tunnel. To maintain security, split tunneling will be disabled. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

Creating a policy to match scenario 3 requires:

- Creating a user group.
- Creating a firewall address for the marketing VLAN.
- Creating an SSL VPN portal.
- Creating a SSL VPN firewall policy for the marketing VLAN.

Using the web-based manager

Creating a User Group

1. Go to **User & Device** > **User** > **User Groups** and select **Create New**.
2. Name the Group **remote access**.
3. Set **Type** as **Firewall**.
4. Highlight **tbrown** on the **Available Users** list.
5. Select the right-pointing arrow to move **tbrown** to the **Members** list.
6. Select **OK**.

The entry **remote access** will now appear on the **Group** list, with **tbrown** listed under **Members**.

Creating a Firewall Address for the marketing VLAN

1. Go to **Policy & Objects** > **Objects** > **Addresses** and select **Create New**. Change the following settings:

Address Name	marketing VLAN
Type	Subnet
Subnet/IP Range	172.20.120.14/255.255.255.0
Interface	marketing

2. Select **OK**.

Creating an SSL VPN Portal

1. Go to **VPN** > **SSL** > **Portals** and select **Create New**. Change the following settings:

Name	marketing-remote
Enable Tunnel Mode	Enable
Enable Split Tunneling	Disable
IP Pools	SSLVPN_TUNNEL_ADDR1
Enable Web Mode	Enable

2. Select **Apply**.

Creating a Firewall Policy

1. Go to **Policy & Objects** > **Policy > IPv4** and select **Create New.**
2. Change the following settings to allow Tom Brown to access the marketing VLAN:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	marketing_laptop
Outgoing Interface	marketing
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **Policy & Objects** > **Policy > IPv4** and create a second policy.
5. Change the following settings to allow Tom Brown to access the Internet through the FortiGate:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	marketing_laptop
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

6. Select **OK**.

The FortiClient SSL VPN tunnel client will also need to be configured, in order for the Tom Brown to connect to the SSL VPN tunnel.

You have now finished creating a policy that matches scenario 4. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

Using the CLI

1. Create the user group for remote users.

```
config user group
   edit remote-access
      set group-type firewall
      set member tbrown
end
```

2. Create a firewall address for the marketing VLAN.

```
config firewall address
   edit marketing_VLAN
      set associated-interface marketing
      set subnet 172.20.120.14 255.255.255.0
end
```

3. Create the SSL VPN web portal.

```
config vpn ssl web portal
   edit marketing-remote
      set allow-access web ftp ssh
      config widget
         edit 1
```

```
            set type tunnel
            set split-tunneling disable
            set ip-pools SSLVPN_TUNNEL_ADDR1
            set auto-connect enable
        end
end
```

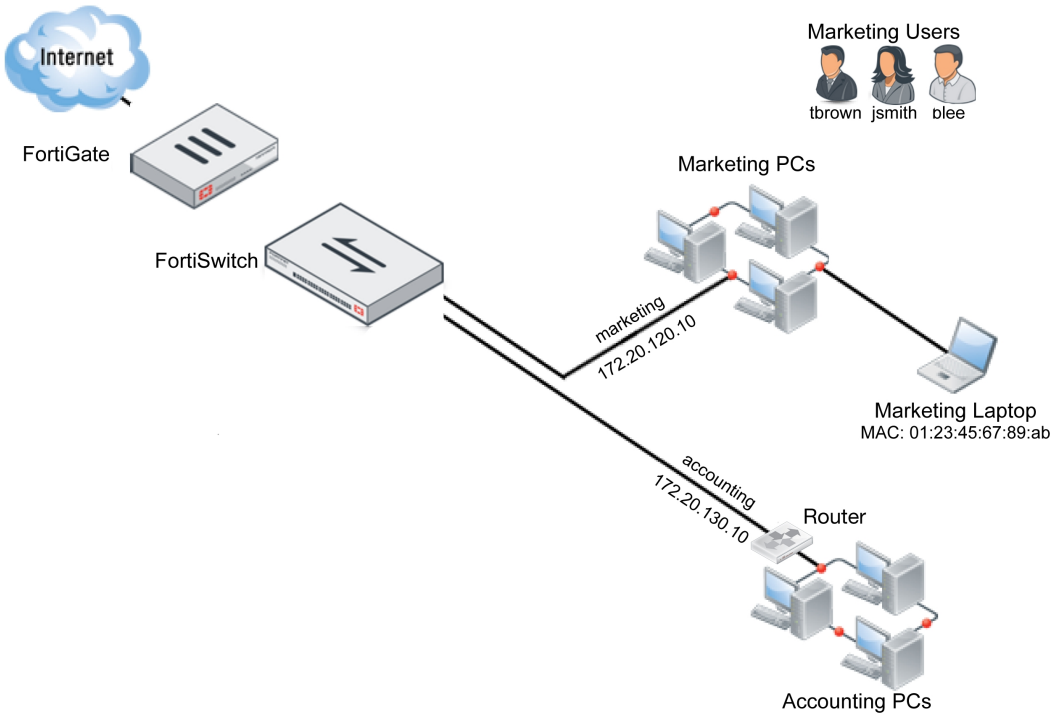
4. Create a firewall policy to allow remote access to the marketing VLAN.

```
config firewall policy
   edit 3
      set srcintf wan1
      set dstintf marketing
      set dstaddr marketing_VLAN
      set action ssl-vpn
      set schedule always
      set groups remote_access
      set users tbrown
      set sslvpn-portal marketing-remote
end
```

Scenario 4: Configuring the accounting VLAN using an SFP port

The SFP ports should only be used to connect UL-listed optical transceiver products, rated Laser Class 1.33V DC.

In Scenario 4, a second VLAN will be created on the FortiSwitch, to be used for the accounting department. This VLAN will connect to the FortiSwitch unit using a copper SFP receiver that has been installed in the FortiSwitch. Due to the sensitive nature of information within the accounting network, the firewall policy that controls traffic to this network uses the default profile for all security features.



Creating an interface to match scenario 4 requires:

- Creating and assigning a VLAN.
- Configuring a firewall policy.

SFP ports are only available on certain FortiSwitch models. SFP ports are also shared with Ethernet ports and so when an SFP port is used, the Ethernet port with the same number cannot be.

Using the web-based manager

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller** > **Switch Network** > **Virtual Switch** and select **Create New**. Change the following settings:

Name	accounting
Color	
IP/Network Mask	172.20.130.15/255.255.255.0

2. Select **OK**.
3. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch** and assign FortiSwitch **port 21** to **accounting**.

Configuring the Firewall Policy

1. Go to **Policy & Objects** > **Policy > IPv4** and select **Create New**. Change the following settings:

Incoming Interface	accounting
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

2. Enable the following Security Profiles and set them to use the **default** profile: **AntiVirus**, **Web Filter**, **Application Control**, **IPS**, **Email Filter**, **DLP Sensor**, and **SSL/SSH Inspection**.
3. Select **OK**.

You have now finished creating a policy that matches scenario 5. This policy will be used for all traffic on the accounting VLAN.

Using the CLI

1. Create the accounting VLAN.

```
config switch-controller vlan
   edit accounting
      set color 32
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.130.15 255.255.255.0
end
```

3. Assign the accounting VLAN to port 21.

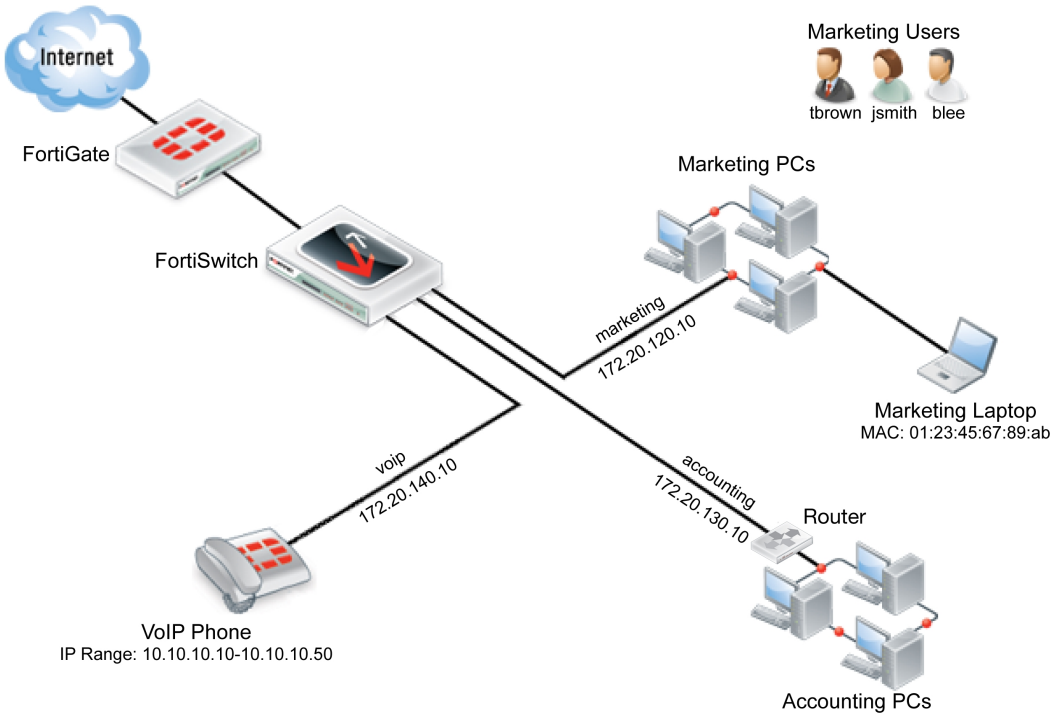
```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port21
            set vlan accounting
      end
end
```

4. Create a firewall policy for the accounting VLAN that uses the default security profiles.

```
config firewall policy
   edit 4
      set srcintf accounting
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set logtraffic all
      set nat enable
      set av-profile default
      set webfilter-profile default
      set spamfilter-profile default
      set dlp-sensor default
      set ips-sensor default
      set application-list default
      set profile-protocol-options default
      set deep-inspection-options default
end
```

Scenario 5: Connecting a VoIP phone to the FortiSwitch

In Scenario 5, an interface will be configured to use a Voice over IP (VoIP) phone. This VoIP phone will be assigned the IP range 10.10.10.10-10.10.10.50 and connect to the FortiSwitch unit through port 10 using an Ethernet cable. The FortiGate unit's default VoIP profile will be used.



Creating an interface to match scenario 5 requires:

- Creating and assigning a VLAN.
- Creating a firewall address for the VoIP phone.
- Configuring a firewall policy.

Using the web-based manager

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller** > **Switch Network** > **Virtual Switch** and select **Create New**. Change the following settings:

Name	voip
Color	
IP/Network Mask	172.20.140.16/255.255.255.0

2. Select **OK**.
3. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch** and assign FortiSwitch **port10** to **voip**.

Creating a Firewall Address

1. Go to **Policy & Objects** > **Objects** > **Addresses** and select **Create New**. Change the following settings:

Category	Address
Name	voip
Color	
Type	IP Range
Subnet/IP Range	10.10.10.10-10.10.10.50
Interface	voip

2. Select **OK**.

Create a Firewall Policy

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**. Change the following settings:

Incoming Interface	voip
Source Address	voip_phone
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	SIP
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

2. Go to **Policy & Objects** > **Policy > IPv4** and select **Create New**. Change the following settings:
3. Enable the **VoIP** Security Profile and set it to **default**.

You have now finished creating a policy that matches scenario 6.

Using the CLI

1. Create the voip VLAN.

```
config switch-controller vlan
   edit voip
      set color 25
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.140.16 255.255.255.0
end
```

3. Assign the voip VLAN to port 10.

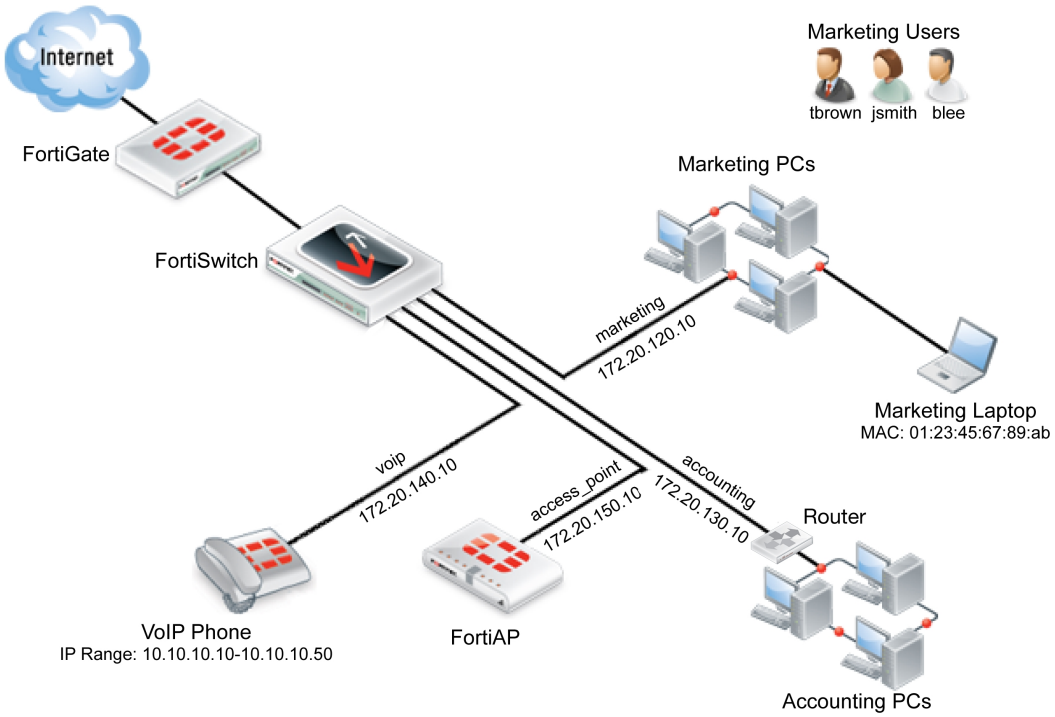
```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port10
            set vlan voip
      end
end
```

4. Configure the firewall policy.

```
config firewall policy
   edit 5
      set srcintf voip
      set dstintf wan1
      set srcaddr voip_phone
      set dstaddr all
      set action accept
      set schedule always
      set service SIP
      set logtraffic all
      set nat enable
      set voip-profile default
end
```

Scenario 6: Connecting a FortiAP unit to the FortiSwitch

In Scenario 6, an interface will be configured to use a FortiAP unit that will provide wireless Internet access.



Creating an interface to match scenario 6 requires:

- Creating and assigning a VLAN.
- Authorizing the FortiAP unit.

- Creating an SSID.
- Creating a firewall address.
- Configuring a firewall policy.

The WiFi network provided by the access point will use the marketing schedule and allow HTTP and HTTPS traffic.

Using the web-based manager

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller** > **Switch Network** > **Virtual Switch** and select **Create New**. Change the following settings:

Name	access_point
Color	
IP/Network Mask	172.20.150.17/255.255.255.0
DHCP Server	Enable

2. Select **OK**.
3. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch** and assign FortiSwitch **port1** to **access_point.**

Authorizing the FortiAP unit

1. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**.
2. Right-click on the FortiAP unit and select **Authorize**.

A icon with a checkmark now appears in the Status column.

Creating an SSID

1. Go to **WiFi & Switch Controller > WiFi Network > SSIDs** and select **Create New.**
2. Change the following settings:

Name	WLAN
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	172.20.150.17/255.255.255.0
DHCP Server	Enabled
SSID	wireless
Pre-shared Key	password

3. Select **OK**.

Create a Firewall Policy

1. Go to **Policy & Objects** > **Policy > IPv4** and select **Create New**.
2. Change the following settings:

Incoming Interface	access_point
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**. The Status icon now appears in green, showing that the FortiSwitch unit is online.

You have now finished creating a policy that matches scenario 7.

Using the CLI

1. Create the access_point VLAN.

```
config switch-controller vlan
   edit access_point
      set color 7
end
```

2. Assign the access_point VLAN to port 1.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port1
            set vlan access_point
      end
end
```

3. Set the interface IP and enable CAPWAP.

```
config system interface
   edit access_point
      set ip 172.20.150.17
      set allowaccess capwap
end
```

4. Enable the FortiAP unit.

```
config wireless-controller wtp
```

```
   edit FAP11C3X13000412
      set admin enable
end
```

5. Create an SSID for the FortiAP unit.

```
config wireless-controller vap
   edit WLAN
      set ssid wireless
      set passphrase password
end
```

6. Configure the firewall policy.

```
config firewall policy
   edit 6
      set srcintf access_point
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP HTTPS DNS
      set logtraffic all
      set nat enable
end
```

Chapter 21 - Security Profiles

This FortiOS Handbook chapter contains the following sections:

Security Profiles overview describes Security Profiles components and their relation to firewall policies, as well as SSL content scanning and inspection. We recommend starting with this section to become familiar with the different features in your FortiGate unit.

Client Reputation explains how to track client behavior and report on activities that you determine are risky or otherwise noteworthy.

AntiVirus explains how the FortiGate unit scans files for viruses and describes how to configure the antivirus options.

Email filter explains how the FortiGate unit filters email, describes how to configure the filtering options and the action to take with email detected as spam.

Intrusion protection explains basic Intrusion Protection System (IPS) concepts and how to configure IPS options; includes guidance and a detailed table for creating custom signatures as well as several examples.

Web filter and FortiGuard Web Filter The first of these sections describes basic web filtering concepts, the order in which the FortiGate unit performs web filtering, and configuration. The second section describes enhanced features of the subscription-based FortiGuard Web Filtering service and explains how to configure them. We recommend reading both sections if you are using FortiGuard Web Filtering because settings you configure in one feature may affect the other.

Data leak prevention describes the DLP features that allow you to prevent sensitive data from leaving your network and explains how to configure the DLP rules, compound rules, and sensors.

Application control describes how your FortiGate unit can detect and take action against network traffic based on the application generating the traffic.

Security Profiles overview

Ranging from the FortiGate®-30 series for small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers, the FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Security Profiles. The Security Profiles features your FortiGate model includes are:

- AntiVirus
- Intrusion Prevention System (IPS)
- Web filtering
- E-mail filtering, including protection against spam and grayware
- Data Leak Prevention (DLP)
- Application Control
- ICAP

Firewall policies limit access, and while this and similar features are a vital part of securing your network, they are not covered in this document.

The following topics are included in this section:

- Traffic inspection
- Content inspection and filtering
- Security Profiles components
- Security Profiles/lists/sensors

Traffic inspection

When the FortiGate unit examines network traffic one packet at a time for IPS signatures, it is performing traffic analysis. This is unlike content analysis where the traffic is buffered until files, email messages, web pages, and other files are assembled and examined as a whole.

DoS policies use traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses.

Application control uses traffic analysis to determine which application generated the packet.

Although traffic inspection doesn't involve taking packets and assembling files they are carrying, the packets themselves can be split into fragments as they pass from network to network. These fragments are reassembled by the FortiGate unit before examination.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats.

IPS signatures

IPS signatures can detect malicious network traffic. For example, the Code Red worm attacked a vulnerability in the Microsoft IIS web server. Your FortiGate's IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions.

IPS recommendations

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new IPS signatures as soon as they are available.
- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to **Block**.
- You can view these signatures by going to **Security Profiles > Intrusion Protection** and selecting the **[View IPS Signatures]** link.
- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to **Block**.

Suspicious traffic attributes

Network traffic itself can be used as an attack vector or a means to probe a network before an attack. For example, SYN and FIN flags should never appear together in the same TCP packet. The SYN flag is used to initiate a TCP session while the FIN flag indicates the end of data transmission at the end of a TCP session.

The FortiGate unit has IPS signatures that recognize abnormal and suspicious traffic attributes. The SYN/FIN combination is one of the suspicious flag combinations detected in TCP traffic by the `TCP.BAD.FLAGS` signature.

The signatures that are created specifically to examine traffic options and settings, begin with the name of the traffic type they are associated with. For example, signatures created to examine TCP traffic have signature names starting with TCP.

Application control

While applications can often be blocked by the ports they use, application control allows convenient management of all supported applications, including those that do not use set ports.

Application control recommendations

- Some applications behave in an unusual manner in regards to application control. For more information, see "Application considerations".
- By default, application control allows the applications not specified in the application control list. For high security networks, you may want to change this behavior so that only the explicitly allowed applications are permitted.

Content inspection and filtering

When the FortiGate unit buffers the packets containing files, email messages, web pages, and other similar files for reassembly before examining them, it is performing content inspection. Traffic inspectionTraff, on the other hand, is accomplished by the FortiGate unit examining individual packets of network traffic as they are received.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats. Be sure to understand the effects of the changes before using the suggestions.

AntiVirus

The FortiGate antivirus scanner can detect viruses and other malicious payloads used to infect machines. The FortiGate unit performs deep content inspection. To prevent attempts to disguise viruseAns, the antivirus scanner will reassemble fragmented files and uncompress content that has been compressed. Patented Compact Pattern Recognition Language (CPRL) allows further inspection for common patterns, increasing detection rates of virus variations in the future.

AntiVirus recommendations

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new antivirus signatures as soon as they are available.
- Enable the Extended Virus Database if your FortiGate unit supports it.
- Examine antivirus logs periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.
- The **builtin-patterns** file filter list contains nearly 20 file patterns. Many of the represented files can be executed or opened with a double-click. If any of these file patterns are not received as a part of your normal traffic, blocking them may help protect your network. This also saves resources since files blocked in this way do not need to be scanned for viruses.
- To conserve system resources, avoid scanning email messages twice. Scan messages as they enter and leave your network or when clients send and retrieve them, rather than both.

FortiGuard Web Filtering

The web is the most popular part of the Internet and, as a consequence, virtually every computer connected to the Internet is able to communicate using port 80, HTTP. Botnet communications take advantage of this open port and use it to communicate with infected computers. FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.

FortiGuard Web Filtering recommendations

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous.
- In the email filter profile, enable **IP Address Check** in **FortiGuard Email Filtering**. Many IP addresses used in spam messages lead to malicious sites; checking them will protect your users and your network.

Email filter

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine. The FortiGate email filter can detect harmful spam and mark it, alerting the user to the potential danger.

Email filter recommendations

- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint scanning for protection against threats that get into your network.
- Subscribe to the FortiGuard AntiSpam Service.

DLP

Most security features on the FortiGate unit are designed to keep unwanted traffic out of your network while DLP can help you keep sensitive information from leaving your network. For example, credit card numbers and social security numbers can be detected by DLP sensors.

DLP recommendations

- Rules related to HTTP posts can be created, but if the requirement is to block all HTTP posts, a better solution is to use application control or the **HTTP POST Action** option in the web filter profile.
- While DLP can detect sensitive data, it is more efficient to block unnecessary communication channels than to use DLP to examine it. If you don't use instant messaging or peer-to-peer communication in your organization, for example, use application control to block them entirely.

Security Profiles components

AntiVirus

Your FortiGate unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support additional virus databases are able to identify hundreds of thousands of viruses. With a FortiGuard AntiVirus subscription, the signature databases are updated whenever a new threat is discovered.

AntiVirus also includes file filtering. When you specify files by type or by file name, the FortiGate unit will stop the matching files from reaching your users.

FortiGate units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files for that you can examine later.

Intrusion Protection System (IPS)

The FortiGate Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures, tailored to your network.

Web filtering

Web filtering includes a number of features you can use to protect or limit your users' activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

Email filtering

FortiGuard AntiSpam is a subscription service that includes an IP address black list, a URL black list, and an email checksum database. These resources are updated whenever new spam messages are received, so you do not need to maintain any lists or databases to ensure accurate spam detection.

You can use your own IP address lists and email address lists to allow or deny addresses, based on your own needs and circumstances.

Data Leak Prevention (DLP)

Data leak prevention allows you to define the format of sensitive data. The FortiGate unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.

Application Control

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1000 applications, improving your control over application communication.

ICAP

This module allows for the offloading of certain processes to a separate server so that your FortiGate firewall can optimize its resources and maintain the best level of performance possible.

Security Profiles/lists/sensors

A profile is a group of settings that you can apply to one or more firewall policies. Each Security Profile feature is enabled and configured in a profile, list, or sensor. These are then selected in a security policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the security policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

While you can apply more than one security profile to a firewall policy, it is not recommended that you use flow-based profiles and proxy-based profiles in the same firewall policy.

Because you can use profiles in more than one security policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you

might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

The Security Profiles include:

- Antivirus profile
- IPS sensor
- Web filter profile
- Email filter profile
- Data Leak Prevention profile
- Application Control list
- VoIP profile

Although they're called profiles, sensors, and lists, they're functionally equivalent. Each is used to configure how the feature works.

AntiVirus

This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unit supports SSL content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.

In many cases you can just customize the default antivirus profile and apply it to the security policy that accepts the traffic to be virus scanned. You can also create custom antivirus profiles if want to apply different types of virus protection to different traffic.

The following topics are included in this section:

- Antivirus concepts
- Enabling AntiVirus scanning
- Testing your antivirus configuration
- Example Scenarios

Antivirus concepts

The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.

The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.

Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

Malware Threats

Viruses

Viruses are self replicating code that install copies of themselves into other programs, data files for boot sectors of storage devices. Virus can often carry a “payload” which performs some undesirable function. These functions can include but are not limited to:

- Stealing drive space
- Stealing cpu cycles
- Accessing private information
- Corrupting data

- Digital defacement or vandalism
- Spamming contact lists

Worms

A worm is a piece of standalone computer code that replicates itself in order to spread to other computers. It normally uses a computer network to spread itself, using security vulnerabilities on the target computer or network to propagate. Unlike a virus, it does not attach itself to an existing file. Even is there is no payload, worms consume resources such as bandwidth and storage space just through their act of replication.

Trojan horses

A Trojan horse, or Trojan is malware that is defined by its delivery method. Through the use of social engineering, or some other method, the code is installed on a system by a valid user of the system and like the original Trojan horse there is something more than advertised within the software. Trojans, unlike worms or viruses are generally non-self-replicating. The most common payload of a Trojan is the setting up of a “backdoor” control mechanism to the system that it is installed on.

Ransomware

Ransomware is a type of malware that, as the name implies, hold the system ransom until payment of some kind is made. It does this by restricting access to the legitimate owner of the system either by encrypting files or locking the system. Usually, a message of some kind is displayed with the demands. Upon payment a utility or key is sent to the user to unlock the system.

Scareware

Scareware comes in two main flavours; the first tries to convince the user that his computer is invected with some non-existent malware, scaring the user into purchasing the author’s virus removal utility. The utility is nonfunctional or some additional form of malware.

The second form tries to convince the user that the computer has been or is being used for an illegal act such as being part of a bot net or storing child pornography. Again, the objective is to scare the user into paying to cure something that is not really there.

Spyware

Spyware is used by its authors to collect information about the user and its computer without the users knowledge. The end result can be as benign as being better able to target adds, to as criminal as key loggers designed to record account ids and passwords of bank accounts and forward them off to the authors.

Adware

Adware is not malware per se. It is merely any software that produces advertisements in order to generate revenue for its author. While a lot of people find this inconvenient or irritating it is not malware. As such it is not blocked by the antivirus software for being malware. This doesn’t mean that software that has adware built into it will not be block if it does have malware in it.

Botnets

A botnet is a network of Internet connected computers that have been covertly usurped to forward transmissions to other computers on the Internet on behalf of a “master”. These transmission can be merely annoying such as spam or they can critically impact a target as when used to launch a Distributed Denial of Service attack.

Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based.

According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

Phishing

Phishing is a social engineering technique that is used to obtain sensitive and confidential information by masquerading as a communication from a trusted entity such as a well known institution, company or website. Usually, the malware is not in the communication itself but in the links within the communication.

Grayware

Grayware programs are unsolicited software programs installed on computers, often without the user’s consent or knowledge. Grayware programs are generally considered an annoyance, but they can also cause system performance problems or be used for malicious purposes.

Scanning Modes

FortiOS has two different mode of scanning for malware. The reasons for the different modes are performance and granularity. In just about everything relating to security there is a constant balancing act going on. As you increase the level of security and comprehensiveness, there is by necessity a decrease in either convenience or performance, sometimes both. The increase in processing to scan for more threats requires more resources; resources that are a finite supply on the hardware. Granularity can sometimes be used to mitigate performance impact by scanning for a smaller subset of traffic but this is only recommended when that smaller subset of traffic is the only traffic going through the firewall.

If the the traffic on the device is slight then the impact on the performance will hardly be noticeable, but it the unit is working close to capacity in terms of traffic and there are a lot of files coming through then there might be a noticeable decline in the performance.

While both modes offer significant security, Proxy-based is weighted towards being more thorough and easily configurable, while Flow-based is designed to optimize performance.

Proxy

The most thorough scan requires that the FortiGate unit have the whole file for the scanning procedure. To achieve this, the antivirus proxy buffers the file as it arrives. Once the transmission is complete, the virus scanner examines the file. If no infection is present, it is sent to the destination. If an infection is present, a replacement message is set to the destination.

During the buffering and scanning procedure, the client must wait. With a default configuration, the file is released to the client only after it is scanned. You can enable client comforting in the Proxy Options profile to feed the client a trickle of data to prevent them from thinking the transfer is stalled, and possibly cancelling the download.

Buffering the entire file allows the FortiGate unit to eliminate the danger of missing an infection due to fragmentation because the file is reassembled before examination. Archives can also be expanded and the contents scanned, even if archives are nested.

Since the FortiGate unit has a limited amount of memory, files larger than a certain size do not fit within the memory buffer. The default buffer size is 10 MB. You can use the uncompsizelimit CLI command to adjust the size of this memory buffer.

Files larger than the buffer are passed to the destination without scanning. You can use the **Oversize File/Email** setting to block files larger than the antivirus buffer if allowing files that are too large to be scanned is an unacceptable security risk.

Flow-based

If your FortiGate unit supports flow-based antivirus scanning, you can select it instead of proxy-based antivirus scanning. The way flow-based antivirus works changed significantly starting with firmware version 5.2. In fact, the new method of flow-based antivirus inspection is sometimes called "deep flow" inspection to differentiate it from the older method.

As packets of a file come into the FortiGate unit, a copy of the packet is cached locally before the packet is allowed to pass through to the recipient. When the last packet of the file arrives, it is also cached but put on hold. Now the entire cached file is delivered to the Antivirus engine for a full scanning, just as it would be if using the proxy-based method, using what ever antivirus database has been configured.

If the file is determined to be infected with malware, the last packet will be dropped and the session is reset. Without all of the packets the file cannot be built by the recipient. When download a file through an HTTP connection (or HTTPS is SSL scanning is enabled), the flow-based feature remembers the last virus result so any subsequent attempts to download the same file will be welcomed by an appropriate blocked message directly, without engaging in the effort of downloading the file.

By using the same engine as the proxy-based method the detection rate is the same for both methods. In terms of performance from the end user's stand point, the performance of the download will be a lot faster until the last packet and then there will be a slight delay for the scan, but after the determination is made only one packet has to be sent from the firewall to the recipient so the overall speed is faster than the proxy based method.

An additional advantage of the flow-based method is that the scanning process does not change the packets as they pass through the FortiGate unit, while proxy-based scanning can change packet details such as sequence numbers. The changes made by proxy-based scanning do not affect most networks.

Antivirus scanning order

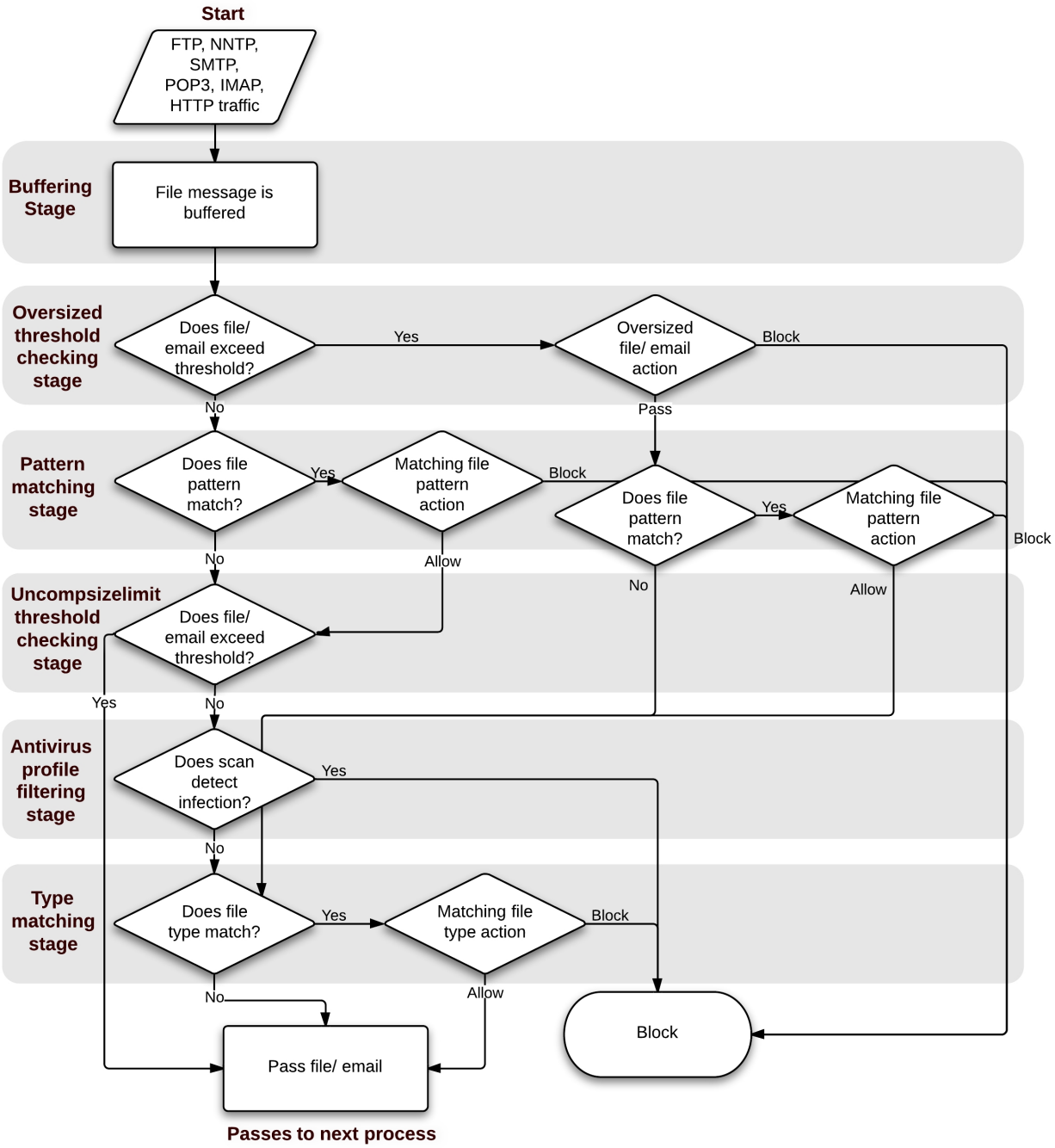
The antivirus scanning function includes various modules and engines that perform separate tasks.

Proxy-based antivirus scanning order

The following figure illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The `uncompsizelimit` check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the `config antivirus service` command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.

File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.

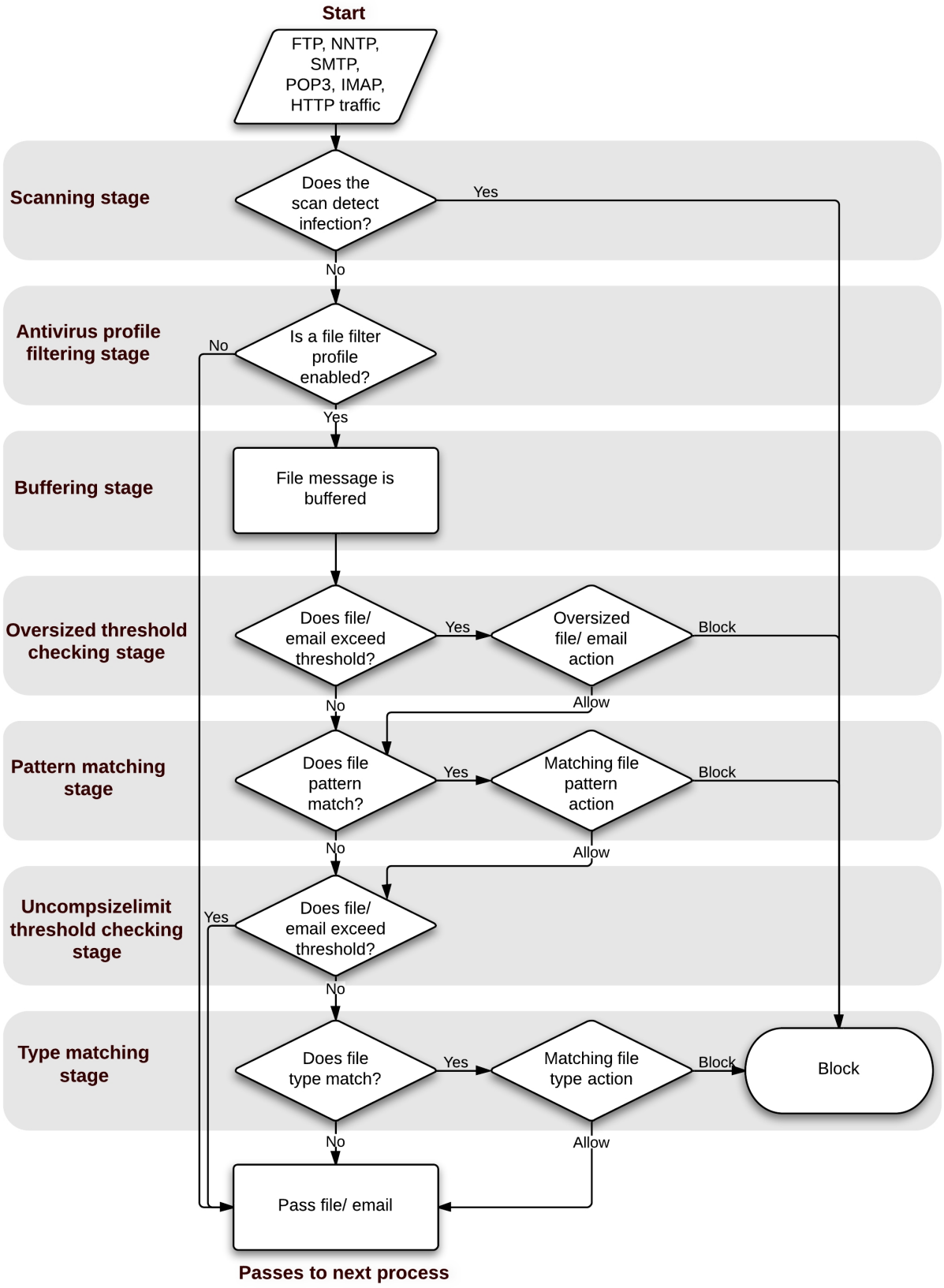
Antivirus scanning order when using the normal, extended, or extreme database



If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file `fakefile.EXE` is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.

Flow-based antivirus scanning order

The following figure illustrates the antivirus scanning order when using flow-based scanning (i.e. the flow-based database). The antivirus scan takes place before any other antivirus-related scan. If file filter is not enabled, the file is not buffered. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.


Start
FTP, NNTP, SMTP, POP3, IMAP, HTTP traffic
Scanning stage
Does the scan detect infection?
Yes
No
Antivirus profile filtering stage
Is a file filter profile enabled?
No
Yes
Buffering stage
File message is buffered
Oversized threshold checking stage
Does file/ email exceed threshold?
Yes
Oversized file/ email action
Block
Allow
No
Pattern matching stage
Does file pattern match?
Yes
Matching file pattern action
Block
Allow
No
Uncompsizelimit threshold checking stage
Does file/ email exceed threshold?
Yes
No
Type matching stage
Does file type match?
Yes
Matching file type action
Block
Block
No
Allow
Pass file/ email
Passes to next process

Antivirus databases

The antivirus scanning engine relies on a database of virus signatures to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.

All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.

Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.

If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, you can select the virus database most suited to your needs.

If you require the most comprehensive antivirus protection, enable the extended virus database. The additional coverage comes at a cost, however, because the extra processing requires additional resources.

To change the antivirus database

Use the CLI to run the following commands:

```
config antivirus settings
   set default-db extended
end
```

Antivirus techniques

The first three antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first two features have specific functions, the third, heuristics, protects against new, or previously unknown virus threats.

To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services.

The Botnet protection looks for links to malware rather than malware itself.

Virus scan

If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN).

Grayware protection

If the file passes the virus scan, it can be checked for grayware.

Grayware scanning is an optional function and must be enabled in the CLI if it is to be scanned for along with other malware. Grayware cannot be scanned for on its own. While done as a separate step, antivirus scanning must be enabled as well.

To enable grayware detection enter the following in the CLI:

```
config antivirus settings
   set grayware enable
end
```

To disable grayware detection enter the following in the CLI:

```
config antivirus settings
   set grayware disable
end
```

Grayware signatures are kept up to date in the same manner as the antivirus definitions.

Heuristics

After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.

To set heuristics, enter the following in the CLI:

```
config antivirus heuristic
   set mode {pass |block |disable}
end
```

- "`block`" enables heuristics and any files determined to be malware are blocked from entering the network.
- "`pass`" enables heuristics but any files determined to be malware are still allowed to pass through to the recipient.
- "`disable`" turns off heuristics.

FortiGuard Antivirus

The FortiGuard Antivirus services are included in the regular FortiGuard subscription and include automatic updates of antivirus engines and definitions as well as a DNS black list (DNSBL) through the FortiGuard Distribution Network (FDN).

Current information about your subscription and version numbers can be found at **System > Config > FortiGuard.** This page will also allow the configuration of connections to the FortiGuard Center and how often to check for updates to the antivirus files.

Botnet protection

Protection from having your system being controlled by a botnet is achieved by detecting and blocking connection attempts to known botnets. This feature also includes connections to known phishing sites. The FortiGuard IP Reputation Database (IRDB) continually updated with addresses of known command and control (C&C) sites that botnet clients attempt to connect to, as well as a database of phishing URLs. Access to this database is available to users through FortiCare support contracts purchased or renewed before October 1, 2016. After that date, users

will have to subscribe to the IRDB either through FortiGuard Mobility Security Service (FMSS) or the FortiGuard Enterprise Bundle.

To enable Botnet and phishing protection in an antivirus profile check the checkbox next to **Detect Connection to Botnet C&C Servers**.

The Botnet protection feature is available for both proxy and flow-based antivirus profiles.

Quarantine / Source IP ban

Starting in FortiOS 5.2, the quarantine, as a place where traffic content was held in storage where it couldn't interact with the network or system was removed, but the term quarantine was kept to describe keeping selected source IPs from interacting with the network and protected systems. This source IP ban is kept in the kernel rather than in any specific application engine and can be queried by APIs. The features that can use the APIs to access and use the banned source IP addresses are antivirus, DLP, DoS and IPS. Both IPv4 and IPv6 version are included in this feature.

To configure the antivirus profile to add the source IP address of an infected file to the quarantine or list of banned source IP addresses edit the Antivirus profile, in the CLI. as follows:

```
config antivirus profile
   edit <name of profile>
      config nac-quar
         set infected quar-src-ip
         set expiry 5m
      end
```

If the `quar-src-ip` action is used, the additional variable of expiry time will become available. This variable determines for how long the source IP adddress will be blocked. In the CLI the option is called `expiry` and the duration is in the format `<###d##h##m>`. The maximum days value is 364. The maximum hour value is 23 and the maximum minute value is 59. The default is 5 minutes.

FortiGuard Sandbox

Not every piece of malware has a signature yet. This is especially true of new malware and new variations on existing malware. FortiOS can upload suspicious files to FortiGuard Sandbox where the file will be executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. The next time your FortiGate unit updates its antivirus database it will have the new signature.

A file is considered suspicious if it does not contain a known virus and if it has some suspicious characteristics. The suspicious characteristics can change depending on the current threat climate and other factors. Fortinet optimizes how files are uploaded as required.

To configure an Antivirus profile to enable the use of the FortiGuard Sandbox check the checkbox next to **Send Files to FortiGuard Sandbox for Inspection (Requires FortiCloud account)**.

Sending files to the FortiGuard Sandbox does not block files that it uploads. Instead they are used to improve how quickly new threats can be discovered and signatures created for them and added to the FortiGuard antivirus database.

The Advanced Threat Protection dashboard widget shows the number of files that your FortiGate unit has uploaded or submitted to FortiGuard Sandbox.

Client Comforting

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit scans it. If no infection is found, the file is sent along to the client. The client initiates the file transfer and nothing happens until the FortiGate finds the file clean, and releases it. Users can be impatient, and if the file is large or the download slow, they may cancel the download, not realizing that the transfer is in progress.

The client comforting feature solves this problem by allowing a trickle of data to flow to the client so they can see the file is being transferred. The default client comforting transfer rate sends one byte of data to the client every ten seconds. This slow transfer continues while the FortiGate unit buffers the file and scans it. If the file is infection-free, it is released and the client will receive the remainder of the transfer at full speed. If the file is infected, the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file.

If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.

Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS and FTPS traffic.

Enable and configure client comforting

1. Go to **Policy & Objects> Policy > Proxy Options**.
2. Select a Proxy Options profile and choose **Edit**, or select **Create New** to make a new one.
3. Scroll down to the **Common Options** section and check the box next to **Comfort Clients**. This will set the option on all of the applicable protocols. The ability to set this feature on a protocol by protocol basis exists in the CLI
4. Select **OK or Apply** to save the changes.
5. Select this Proxy Options profile in any security policy for it to take effect on all traffic handled by the policy.

The default values for Interval and Amount are 10 and 1, respectively. This means that when client comforting takes effect, 1 byte of the file is sent to the client every 10 seconds. You can change these values to vary the amount and frequency of the data transferred by client comforting.

Oversized files and emails

Downloaded files can range from a few Kilobytes to multiple Gigabytes. The problem lies in that a FortiGate doesn't have the memory to allow for a large number of people downloading large files. Image the memory required for a team of developers to all download the latest Linux OS distribution at once, in addition to the normal requirements of the firewall. Everything would come to a grinding halt the FortiGate tried to store each of those Gibabyte+ files in memory. To give you some piece of mind, the chances of malware being in a large file like those is much smaller than in a smaller single Megabyte file, so the threat is somewhat limited, but you will probably want to use your computers antivirus software to scan those large files after they have been downloaded.

Therefore a threshold must be set to prevent the resources of the system from becoming overloaded. By default the threshold is 10 MB. Any files larger than the threshold will not be scanned for malware. With a maximum file size threshold in place, it must now be determined what is to be done with the files that are larger than threshold. There are only 2 choices; either the file is passed through without being scanned for malware or the file is blocked. The default action for oversized files is to pass them through.

If you wish to block the downloading of files over the threshold, this can be set within the Proxy Option profile found at **Policy & Objects > Policy > Proxy Options**, under **Common Options**.

Check Block Oversized File/Email

This will reveal an additional option, Threshold (MB). The threshold of the files is set based upon the protocol being used to transfer the file. In the CLI and configuration file, the threshold variable is found in each of the protocol sections within the profile. Changing the value in this field will change the `oversize-limit` value for all of the protocols.

If you wish to change the oversize-limit value on all of the protocols covered in a Proxy Option profile you have two options.

1. You can go into the CLI and change the value manually within each of the protocol sections.
2. You can use the GUI to temporarily block oversized files, and when configuring it change the threshold to the new value that you want. Apply this setting. Then go back to the profile and turn off the block setting. If you now go into the CLI you will find that the configuration file has retained the new oversize-limit value.

The settings can be found in the CLI by going to:

```
config firewall profile-protocol-options
   edit <the name of the profile>
```

Archive scan depth

The antivirus scanner will open archives and scan the files inside. Archives within other archives, or nested archives, are also scanned to a default depth of twelve nestings. You can adjust the number of nested archives to which the FortiGate unit will scan with the uncompressed-nest-limit CLI command. Further, the limit is configured separately for each traffic type.

Configuring archive scan depth

For example, this CLI command sets the archive scan depth for SMTP traffic to 5. That is, archives within archives will be scanned five levels deep.

config firewall profile-protocol-options

```
edit "default"
   config http
      set uncompressed-nest-limit 5
   end
```

You can set the nesting limit from 2 to 100.

Scan buffer size

When checking files for viruses, there is a maximum file size that can be buffered. Files larger than this size are passed without scanning. The default size for all FortiGate models is 10 megabytes.

Archived files are extracted and email attachments are decoded before the FortiGate unit determines if they can fit in the scan buffer. For example, a 7 megabyte ZIP file containing a 12 megabyte EXE file will be passed

without scanning with the default buffer size. Although the archive would fit within the buffer, the uncompressed file size will not.

Configuring the uncompression buffer

In this example, the `uncompressed-oversize-limit` CLI command is used to change the scan buffer size to 20 megabytes for files found in HTTP traffic:

config firewall profile-protocol-options

```
edit "default"
   config http
      set uncompressed-oversize-limit 20
   end
```

The maximum buffer size varies by model. Enter `set uncompressed-oversize-limit ?` to display the buffer size range for your FortiGate unit.

Windows file sharing (CIFS)

FortiOS supports virus scanning of Windows file sharing traffic. This includes CIFS, SMB, and SAMBA traffic. This feature is applied by enabling SMB scanning in an antivirus profile and then adding this profile to a security policy that accepts CIFS traffic. CIFS virus scanning is available only through flow-based antivirus scanning.

FortiOS flow-based virus scanning can detect the same number of viruses in CIFS/SMB/SAMBA traffic as it can for all supported content protocols.

Note the following about CFIS/SMB/SAMBA virus scanning:

- Some newer version of SAMBA clients and SMB2 can spread one file across multiple sessions, preventing some viruses from being detected if this occurs.
- Enabling CIFS/SMB/SAMBA virus scanning can affect FortiGate performance.
- SMB2 is a new version of SMB that was first partially implemented in Windows Vista.
- Currently SMB2 is supported by Windows Vista or later, and partly supported by Samba 3.5 and fully support by Samba 3.6.
- The latest version of SMB2.2 will be introduced with Windows 8.
- Most clients still use SMB as default setting.

Configuring CIFS/SMB/SAMBA virus scanning

Use the following command to enable CIFS/SMB/SAMBA virus scanning in an antivirus profile:

```
config antivirus profile
   edit <smb-profile>
      config smb
         set options scan
      end
```

Then add this antivirus profile to a security policy that accepts the traffic to be virus scanned. In the security policy the service can be set to ANY, SAMBA, or SMB.

```
config firewall policy
   edit 0
      set service ANY
      ...
      set utm-status enable
      set av-profile <smb-profile>
```

```
end
```

Enabling AntiVirus scanning

Antivirus scanning is configured in an antivirus profile, but it is enabled in a firewall policy. Once the use of an antivirus profile is enabled and selected in one or more firewall policies, all the traffic controlled by those firewall policies will be scanned according to the settings in that profile.

In the Feature section found by going to **System > Config > Features,** you can enable or disable 2 aspects of the Antivirus Profile.

1. Antivirus will determine if the option to use Antivirus profiles is available.
2. Multiple Security Profiles will determine if you can configure any Antivirus profiles beyond the default profile.

The **Feature** section can sometimes be misunderstood as to its actual effect. The enabling or disabling of a feature in this section refers to its visibility within the GUI, not whether or not the feature's functionality will work. If you were to disable the Antivirus Profile feature it would disappear from the GUI but not the CLI and configuration file. Since the functionality of the FortiGate unit is based on the contents of the config file any profile referred to by the policy in the configuration will be acted upon. The Feature section is primarily for keeping the GUI clean and uncluttered by features that are not being used by the administrators.

As the use of antivirus these days is practically a minimum standard for security protection the question left to decide is whether or not you wish to use multiple profiles in your configuration.

Antivirus profiles

From **Security Profiles > Antivirus** you can edit existing profiles or create and configure new antivirus profiles that can then be applied to firewall policies. A profile is specific configuration information that defines how the traffic within a firewall policy is examined and what action may be taken based on the examination.

You can create multiple antivirus profiles for different antivirus scanning requirements. For example, you create an antivirus profile that specifies only virus scanning for POP3 which you then apply to the out-going firewall policy that is designed for users getting their email from the mail server. You can also choose specific protocols, such as HTTP, that will be scanned and if blocked, archived by the unit. This option is available only in the CLI.

Whether the mode of the antivirus detection is proxy-based or flow-based is also set within the profile.

Enable Antivirus steps - GUI based

1. Go to **Security Profiles > AntiVirus**.
2. Choose whether you want to edit an exiting profile or create a new one.
   - The default profile will be the one displayed by default.
   - If you are going to edit an existing profile, selecting it can be done by either using the drop down menu in the upper right hand corner of the window or by selecting the List icon (the furthest right of the 3 icons in the upper right of the window, if resembles a page with some lines on it), and then selecting the profile you want to edit from the list.
   - If you need to create a new profile you can either select the Create New icon (a plus sign within a circle) or select the List icon and then select the Create New link in the upper left of the window that appears.
3. If you are creating a new profile, write a name for it in the Name field.
4. Add or edit the Comments fields to more clearly describe the function.
5. Select the Inspection Mode.

6. For the Detect Viruses field, select either Block to prevent infected files from passing throughout the FortiGate or Monitor to allow infected files to pass through the FortiGate but to record instances of infection.
7. If you have a FortiCloud account, you can select **Send Files to FortiGuard Sandbox for Inspection (Requires FortiCloud account)**
   - **You can select whether to send All Files** to the Sandbox or **Suspicious Files Only.**
8. If you wish to use the Botnet feature, you can select Detect Connections to Botnet C&C Servers
   - Just like with the viruses, you can select whether to Block or Monitor the files that contain botnet or phishing connections.
9. Select **OK** or **Apply**.
10. Add the Antivirus profile to a firewall security policy.

Enable Antivirus steps - CLI based

You need to configure the scan option for each type of traffic you want scanned.

1. Configure the Antivirus profile

```
config antivirus profile
   edit "default"
      set comment "scan and delete virus"
      set replacemsg-group ''
      set scan-botnet-connections block
      set ftgd-analytics suspicious
      config http
         set options scan
         end
      config ftp
         set options scan
         end
      config imap
         set options scan
         end
      config pop3
         set options scan
         end
      config smtp
         set options scan
         end
      config nntp
         set options scan
         end
      config smb
         set options scan
         end
      end
```

2. Add the Antivirus profile to the Fortigate firewall security policy. When using the CLI, you will need to know the policy ID number.

```
config firewall policy
   edit <policy ID number>
      set av-profile default
      set profile-protocol-options default
      end
```

Testing your antivirus configuration

You have configured your FortiGate unit to stop viruses, but you'd like to confirm your settings are correct. Even if you have a real virus, it would be dangerous to use for this purpose. An incorrect configuration will allow the virus to infect your network.

To solve this problem, the European Institute of Computer Anti-virus Research has developed a test file that allows you to test your antivirus configuration. The EICAR test file is not a virus. It can not infect computers, nor can it spread or cause any damage. It's a very small file that contains a sequence of characters. Your FortiGate unit recognizes the EICAR test file as a virus so you can safely test your FortiGate unit antivirus configuration.

Go to http://www.fortiguard.com/antivirus/eicartest.html to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip).

If the antivirus profile applied to the security policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected.

Example Scenarios

The following examples provide a sample antivirus configuration scenarios.

Configuring simple default antivirus profile

The Antivirus function is so straight forward and widely used that many users just create one default profile and use that on all of the applicable firewall policies. If performance is not a real concern and the unit's resources are not being stretched, it is perfectly reasonable to create one profile that covers the range of uses found in your environment. This example is one possible default configuration.

Context:

- This is an edited default profile and will be used on all security policies
- It will need to scan for malware on all available protocols.
- Malware, botnets, and grayware should be blocked
- The inspection method should be flow-based
- A current FortiCloud account is available

Creating the profile - GUI

1. In the following fields, enter the indicated values or selections:

Name	default
Comments	Scans all traffic from Internet for malware
Inspection Mode	Flow-based
Detect Virus	Block
Send Files to FortiGuard Sandbox for Inspection	checked

• **Suspicious Files Only**	checked
Detect Connections to Botnet C&C Servers	checked
• **Block**	checked

2. Check the appropriate protocols:

Protocol	Virus Scan and Block
HTTP	checked
SMTP	checked
POP3	checked
IMAP	checked
MAPI	checked
FTP	checked
NNTP	checked

3. Select **Apply**.
4. Enable grayware scanning

```
config antivirus settings
   set grayware enable
   end
```

Creating the profile - CLI

1. Enter the CLI by one of the following methods:
   - SSH through a terminal emulator
   - CLI Console widget
   - FortiExplorer's CLI mode
2. Enter the following commands:

```
config antivirus profile
   edit default
      set comment "scan and delete virus"
      set inspection-mode flow-based
      set scan-botnet-connections block
      set ftgd-analytics suspicious
      config http
         set options scan
         end
      config ftp
         set options scan
         end
      config imap
         set options scan
         end
```

```
config pop3
   set options scan
   end
config smtp
   set options scan
   end
config nntp
   set options scan
   end
config smb
   set options scan
   end
end
```

3. Enable grayware scanning

```
config antivirus settings
   set grayware enable
   end
```

Setting up a basic proxy-based Antivirus profile for email traffic

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antivirus protection on a FortiGate unit located in a satellite office.

Context:

- The satellite office does not have an internal email server. To send and retrieve email, the employees connect to an external mail server.
- There is a specific firewall security profile that handles the email traffic from the Internet to the mail server. The only traffic on this policy will be POP3 and IMAP and SMTP
- The company policy is to block viruses and connections to botnets.
- The FortiGate unit is a small model and the Internet bandwidth is limited so the policy is to not submit files to the FortiGuard Sandbox.

Creating the profile - GUI

1. In the following fields, enter the indicated values or selections:

Name	email-av
Comments	Scans email traffic from Internet for malware
Inspection Mode	Proxy
Detect Virus	Block
Send Files to FortiGuard Sandbox for Inspection	checked
• **Suspicious Files Only**	checked
Detect Connections to Bot-net C&C Servers	checked
• **Block**	checked

2. Check the appropriate protocols:

Protocol	Virus Scan and Block
HTTP	checked
SMTP	checked
POP3	checked
IMAP	checked
MAPI	checked
FTP	checked
NNTP	checked

3. Select **Apply**.

Creating the profile - CLI

1. Enter the CLI by one of the following methods:
   - SSH through a terminal emulator
   - CLI Console widget
   - FortiExplorer's CLI mode
2. Enter the following commands:

```
Config antivirus profile
   edit "email-av"
      set comment "Scans email traffic from Internet for malware"
      set inspection-mode proxy
      config imap
         set options scan
         end
      config pop3
         set options scan
         end
      config smtp
         set options scan
         end
      end
```

Adding the profile to a policy

In this scenario the following assumptions will be made:

- The policy that the profile is going to be added to is an IPv4 policy.
- The ID number of the policy is 11.
- The Antivirus profile being added will be the "default" profile
- The SSL/SSH Inspection profile used will be the "default" profile

Adding the profile - GUI

1. Go to **Policy & Objects > Policy > IPv4**.
2. Use your preferred method of finding a policy.
   - If the ID column is available you can use that.
   - You can also choose based on your knowledge of the parameters of the policy
   - Select the policy with ID value of 11
3. In the Edit Policy window, go to the Security Profiles section
4. Turn ON AntiVirus, and in the drop down menu for the field, select default
5. If the AntiVirus profile is proxy-based the Proxy Options field and drop down menu will be revealed.
6. The SSL/SSH Inspection field will automatically be set to ON and one of the profiles will need to be selected from the drop down menu. In this case default is selected.
7. The log options will depend on your requirements and resources but to verify that everything is working properly, it is a good idea to turn ON logging of All Sessions after setting up a new profile and after giving some time for logs to accumulate
8. Turn on Antivirus.
9. Select an antivirus profile.
10. Select **OK** to save the security policy.

Adding the profile - CLI

To select the antivirus profile in a security policy — CLI

```
config firewall policy
   edit 11
      set utm-status enable
      set profile-protocol-options default
      set av-profile basic_antivirus
   end
```

Block files larger than 8 MB

Set proxy options profile to block files larger than 8 MB

1. Go to **Policy & Objects > Policy > Proxy Options**.
2. Edit the default or select Create New to add a new one.
3. Scroll down to the common Options Section and place a check in the box next to BlockOversized File/Email
4. The sub line Threshold (MB) will appear with a value field. Enter 8.
5. Select **OK** or **Apply**.

The proxy options profile is configured, but to block files, you must select it in the firewall policies handling the traffic that contains the files you want blocked.

To select the Proxy Options profile in a security policy

1. Go to **Policy & Objects > Policy > IPv4** (or **IPv6**, depending).
2. Edit or create a security policy.

3. Select a proxy-based security profile. You will know that there is a proxy component to the Security Profile because when a Security Profile is Proxy based the Proxy Options field will be visible (for example, select an Antivirus profile that includes proxy scanning).
4. Beside Proxy Options select the name of the MTU proxy options protocol.
5. Select **OK** to save the security policy.
6. Once you complete these steps, any files in the traffic subject to Security Profile scanning handled by this policy that are larger than 8MB will be blocked. If you have multiple firewall policies, examine each to determine if you want to apply similar file blocking the them as well.

Web filter

This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.

The following topics are included in this section:

- Web filter concepts
- Inspections Modes
- FortiGuard Web Filtering Service
- Overriding FortiGuard website categorization
- SafeSearch
- YouTube Education Filter
- Static URL Filter
- Web content filter
- Advanced web filter configurations
- Configuring Web Filter Profiles
- Web filtering example

Web filter concepts

Web filtering is a means of controlling the content that an Internet user is able to view. With the popularity of web applications, the need to monitor and control web access is becoming a key component of secure content management systems that employ antivirus, web filtering, and messaging security. Important reasons for controlling web content include:

- lost productivity because employees are accessing the web for non-business reasons
- network congestion — when valuable bandwidth is used for non-business purposes, legitimate business applications suffer
- loss or exposure of confidential information through chat sites, non-approved email systems, instant messaging, and peer-to-peer file sharing
- increased exposure to web-based threats as employees surf non-business-related web sites
- legal liability when employees access/download inappropriate and offensive material
- copyright infringement caused by employees downloading and/or distributing copyrighted material.

As the number and severity of threats increase on the World Wide Web, the risk potential increases within a company's network as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation as hostile environments have been created by employees who download and view offensive content. Web-based attacks and threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:

- spyware/grayware
- phishing

- pharming
- instant messaging
- peer-to-peer file sharing
- streaming media
- blended network attacks.

Spyware, also known as grayware, is a type of computer program that attaches itself to a user's operating system. It does this without the user's consent or knowledge. It usually ends up on a computer because of something the user does such as clicking on a button in a pop-up window. Spyware can track the user's Internet usage, cause unwanted pop-up windows, and even direct the user to a host web site. For further information, visit the FortiGuard Center.

Some of the most common ways of grayware infection include:

- downloading shareware, freeware, or other forms of file-sharing services
- clicking on pop-up advertising
- visiting legitimate web sites infected with grayware.

Phishing is the term used to describe attacks that use web technology to trick users into revealing personal or financial information. Phishing attacks use web sites and email that claim to be from legitimate financial institutions to trick the viewer into believing that they are legitimate. Although phishing is initiated by spam email, getting the user to access the attacker's web site is always the next step.

Pharming is a next generation threat that is designed to identify and extract financial, and other key pieces of information for identity theft. Pharming is much more dangerous than phishing because it is designed to be completely hidden from the end user. Unlike phishing attacks that send out spam email requiring the user to click to a fraudulent URL, pharming attacks require no action from the user outside of their regular web surfing activities. Pharming attacks succeed by redirecting users from legitimate web sites to similar fraudulent web sites that have been created to look and feel like the authentic web site.

Instant messaging presents a number of problems. Instant messaging can be used to infect computers with spyware and viruses. Phishing attacks can be made using instant messaging. There is also a danger that employees may use instant messaging to release sensitive information to an outsider.

Peer-to-peer (P2P) networks are used for file sharing. Such files may contain viruses. Peer-to-peer applications take up valuable network resources and may lower employee productivity but also have legal implications with the downloading of copyrighted or sensitive company material.

Streaming media is a method of delivering multimedia, usually in the form of audio or video to Internet users. Viewing streaming media impacts legitimate business by using valuable bandwidth.

Blended network threats are rising and the sophistication of network threats is increasing with each new attack. Attackers learn from each previous successful attack and enhance and update attack code to become more dangerous and fast spreading. Blended attacks use a combination of methods to spread and cause damage. Using virus or network worm techniques combined with known system vulnerabilities, blended threats can quickly spread through email, web sites, and Trojan applications. Examples of blended threats include Nimda, Code Red, Slammer, and Blaster. Blended attacks can be designed to perform different types of attacks, which include disrupting network services, destroying or stealing information, and installing stealthy backdoor applications to grant remote access.

Different ways of controlling access

The methods available for monitoring and controlling Internet access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control web activity.

Common web access control mechanisms include:

- establishing and implementing a well-written usage policy in the organization on proper Internet, email, and computer conduct
- installing monitoring tools that record and report on Internet usage
- implementing policy-based tools that capture, rate, and block URLs.

The final method is the focus of this topic. The following information shows how the filters interact and how to use them to your advantage.

Order of web filtering

The FortiGate unit applies web filters in a specific order:

1. URL filter
2. FortiGuard Web Filter
3. web content filter
4. web script filter
5. antivirus scanning.

If you have blocked a FortiGuard Web Filter category but want certain users to have access to URLs within that pattern, you can use the **Override** within the FortiGuard Web Filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, if you want a user to be able to access www.example.com for one hour, you can use the override to set up the exemption. Any user listed in an override must fill out an online authentication form that is presented when they try to access a blocked URL before the FortiGate unit will grant access to it. For more information, see “FortiGuard Web Filter”.

Inspection Modes

Proxy

Proxy-based inspection involves buffering the traffic and examining it as a whole before determining an action. The process of having the whole of the data to analyze allow this process to include more points of data to analyze than the flow-based or DNS methods.

The advantage of a proxy-based method is that the inspection can be more thorough than the other methods, resulting in fewer false positive or negative results in the analysis of the data.

Flow-based

The Flow-based inspection method examines the file as it passes through the FortiGate unit without any buffering. As each packet of the traffic arrives it is processed and forwarded without waiting for the complete file or web page, etc.

The advantage of the flow-based method is that the user sees a faster response time for HTTP requests and there is less chance of a time-out error due to the server at the other end responding slowly.

The disadvantages of this method are that there is a higher probability of a false positive or negative in the analysis of the data and that a number of points of analysis that can be used in the proxy-based method are not available in the flow-based inspection method. There is also fewer actions available to choose from based on the categorization of the website by FortiGuard services.

DNS

The DNS inspection method uses the same categories as the FortiGuard Service. It is lightweight in terms of resource usage because it doesn't involve any proxy-based or flow-based inspection.

A DNS request is typically the first part of any new session to a new website. This inspection method takes advantage of that and places the results of the categorization of websites right on the FortiGuard DNS servers. When the FortiGate resolves a URL, in addition to the IP address of the website it also receives a domain rating.

In the same way that the flow-based inspection method had fewer filters and points of analysis than the proxy-based inspection method, DNS has fewer settings still. All of its inspection is based on the IP address, the domain name and the rating provided by the FortiGuard DNS server.

If the DNS mode is chosen, the additional setting of a DNS action must be chosen. The options are:

- Block - The traffic will be blocked and the session dropped.
- Redirect - The session will be redirected to a message page indicating to the user what is happening.

FortiGuard Web Filtering Service

FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface.

FortiGuard Web Filter includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.

Before you begin to use the FortiGuard Web Filter options you should verify that you have a valid subscription to the service for your FortiGate firewall.

FortiGuard Web Filter and your FortiGate unit

When FortiGuard Web Filter is enabled in a web filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the FortiGate unit provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

FortiGuard Web Filter Actions

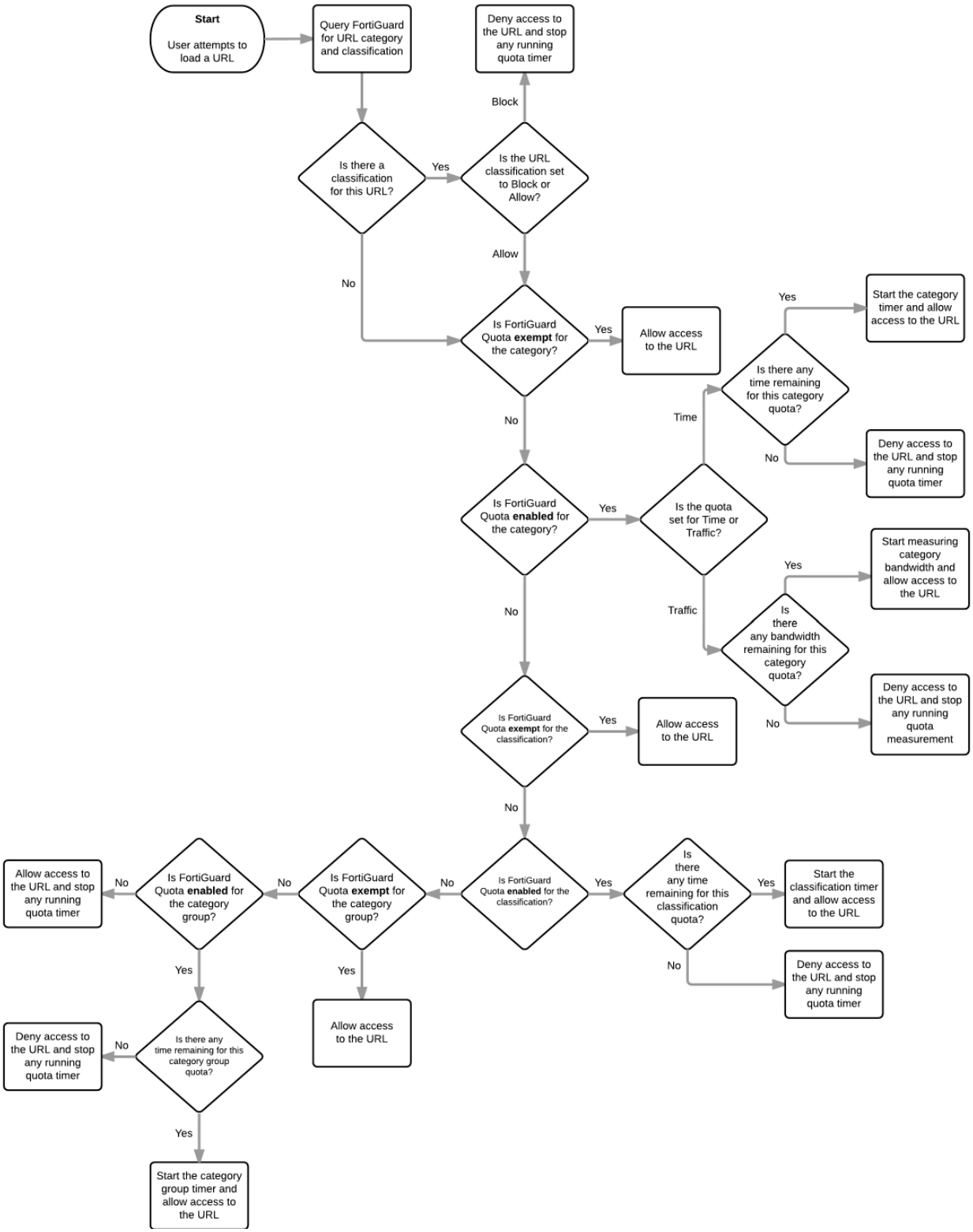
The Possible Actions are:

- **Allow** permits access to the sites within the category.
- **Monitor** permits and logs access to sites in the category. You may also enable user quotas when enabling the monitor action.
- **Warning** presents the user with a message, allowing them to continue if they choose.
- **Authenticate** requires a user authenticate with the FortiGate unit before being allowed access to the category or category group.
- **Block** prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.

The choices of actions available will depend on the mode of inspection.

- Proxy - Allow, Block, Monitor, Warning, Authenticate & Disable.
- Flow-based - Allow, Block & Monitor.
- DNS - Allow, Block & Monitor.

Webfiltering flowchart



FortiGuard Web Filter usage quotas

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily timed access quota by category, category group, or classification. Quotas allow access for a specified length of time or a specified traffic bandwidth, calculated separately for each user. Quotas are reset every day at midnight.

Users must authenticate with the FortiGate unit. The quota is applied to each user individually so the FortiGate must be able to identify each user. One way to do this is to configure a security policy using the identity based policy feature. Apply the web filter profile in which you have configured FortiGuard Web Filter and FortiGuard Web Filter quotas to such a security policy.

The use of FortiGuard Web Filter quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a security policy in which user authentication is not required.

When a user first attempts to access a URL, they're prompted to authenticate with the FortiGate unit. When they provide their user name and password, the FortiGate unit recognizes them, determines their quota allowances, and monitors their web use. The category and classification of each page they visit is checked and FortiGate unit adjusts the user's remaining available quota for the category or classification.

Editing the web filter profile resets the quota timers for all users.

Quota hierarchy

You can apply quotas to categories and category groups. Only one quota per user can be active at any one time. The one used depends on how you configure the FortiGuard Web Filter.

When a user visits a URL, the FortiGate unit queries the FortiGuard servers for the category of the URL. From highest to lowest, the relative priority of the quotas are:

1. Category
2. Category group

Overriding FortiGuard website categorization

In most things there is an exception to the rule. When it comes to the rules about who is allowed to go to which websites in spite of the rules or in this case, policies, it seems that there are more exceptions than to most rules. There are numerous valid reasons and scenarios for exceptions so it follows that there needs to be a way to accommodate this exceptions.

The different methods of override

There are actually two different ways to override web filtering behavior based on FortiGuard categorization of a websites. The second method has 2 variations in implementation and each of the three has a different level of granularity.

1. Using Alternate Categories

   Rating Override

This method manually assigns a specific website to a different Fortinet category or a locally created category.

2. Using Alternate Profiles

   Administrative Override or Allow Blocked Override

   In this method all of the traffic going through the FortiGate unit, using identity based policies and a Web Filtering profile has the option where configured users or IP addresses can use an alternative Web Filter profile when attempting to access blocked websites.

Using Alternate Categories

Web Rating Overrides

There are two approached to overriding the FortiGuard Web Filtering. The first is an identity based method that can be configured using a combination of identity based policies and specifically designed webfilter profiles. This has been addressed in the Firewall Handbook.

The second method is the system wide approach that locally (on the FortiGate Firewall) reassigns a URL to a different FortiGuard Category and even subcategory. This is where you can set assign a specific URL to the FortiGuard Category that you want to you can also set the URL to one of the Custom Categories that you have created

The Web Rating Overrides option is available because different people will have different criteria for how they categorize websites. Even is the criteria is the same an organization may have reason to block the bulk of a category but need to be able to access specific URLs that are assigned to that category.

A hypothetical example could be that a website, example.com is categorized as being in the Sub-Category Pornography. The law offices of Barrister, Solicitor and Lawyer do not want their employees looking at pornography at work so they have used the FortiGuard Webfilter to block access to sites that have been assigned to the Category “Pornography”. However, the owners of example.com are clients of the law office and they are aware that example.com is for artists that specialize in nudes and erotic images. In this case to approaches can be taken. The first is that the Rating Override function can be used to assign example.com to Nudity and Risque instead of Pornography for the purposes of matching the criteria that the law office goes by or the site can be assigned to a Custom Category that is not blocked because the site belongs to one of their clients and they always want to be able to access the site.

Another hypothetical example from the other side of the coin. A private school has decided that a company that specializes in the online selling of books that could be considered inappropriate for children because of their violent subject matter, should not be accessible to anyone in the school. The categorization by Fortinet of the site example2.com is General Interest - Business with the subcategory of Shopping and Auction, which is a category that is allowed at the school. In this case they school could reassign the site to the Category Adult Material which is a blocked category.

Local or Custom Categories

User-defined categories can be created to allow users to block groups of URLs on a per-profile basis. The categories defined here appear in the global URL category list when configuring a web filter profile. Users can rate URLs based on the local categories.

Users can create user-defined categories then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

The local assignment of a category overrides the FortiGuard server ratings and appear in reports as “Local” Categories or “Custom” Categories depending on the context.

In the CLI, they are referred to as Local categories.

To create a Local Category:

```
config webfilter ftgd-local-cat
   edit local_category_1
      set id 140
   end
```

In the GUI they are referred to as Custom Categories. There is a way to create a new category in the Web Based Manager.

1. Go to **Security Profiles** > **Advanced** > **Web Rating Overrides**.
2. Instead of creating a new override, you can choose the “**Custom Categories**” icon in the top menu bar.
3. From the new window select **Create New**.
4. A new row will appear at the bottom of the list of categories with a field on the left highlighted and the message “**This field is required**”. Enter the name of the custom category in this field.
5. Select **Enter**.

Configuring Rating Overrides

1. Go to **Security Profiles** > **Web Filter** > **Web Rating Overrides.**
2. Select **Create New**
3. Type in the **URL** field the URL of the Website that you wish to recategorize.
4. Select the **Lookup Rating** button to verify the current categorization that is being assigned to the URL.
5. Change the **Category** field to one of the more applicable options from the drop down menu.
6. Change the **Sub-Category** field to a more narrowly defined option within the main category.
7. Select **OK**.

It is usually recommended that you choose a category that you know will be addressed in existing Webfilter profiles so that you will not need to engage in further configuration.

Local Category Scenarios

Scenario 1: The configuration of the domain name overrides the configuration for the subdirectory.

Depending on the URL specified or other aspects of configuration, the configuration of a local or custom category may not take effect. Consider a scenario where you have defined:

- example.com – local rating as “category 1”, action set to Block
- example.com/subdirectory – local rating as “category 2”, action set to Monitor
- example.com/subdirectory/page.html – local rating as “category 3”, action set to Warning

If a user browses to “example.com", access will be blocked. If a user browses to example.com/subdirectory, access will also be blocked,even though that address was configured to be part of category2. The configuration of the domain name overrides the configuration for the subdirectory.

However, if you configure a specific HTML page differently than the domain name, then that

configuration will apply. In this scenario, the user will see a Warning message but will be able to pass through to the page.

Scenario 2: User-defined local ratings and SNI matches

In this scenario, local categories are defined and sites are added to those categories.

- There is no behavioral difference if the hostname is sent from from ClientHello SNI or from HTTP request-url.
- The SNI will be used as hostname for https certificate-inspection or ssl-exempt.
- If a valid SNI exist, then SNI will be used as the domain name for url rating instead of CN in the server certificate.
- For the local rating, "example.com" will match "test.example.com", but will not match "another_example.com".

Using Alternate Profiles

Allow Blocked Overrides or Web Overrides

The Administrative Override feature for Web Filtering was added and is found by going to **Security Profiles > Web Filter** and then enabling Allow Blocke Override. This opening window will display a listing of all of the overrides of this type. The editing window referred to the configuration as an Administrative Override.

The Concept

When a Web filter profile is overridden it does not necessarily remove all control and restrictions that were previously imposed by the Web Filter. The idea is to replace a restrictive filter with a different one. In practice, it makes sense that this will likely be a profile that is less restrictive the the original one but there is nothing that forces this. The degree to which that the alternate profile is less restrictive is open. It can be as much as letting the user access everything on the Internet or as little as allowing only one addition website. The usual practice though is to have as few alternate profiles as are needed to allow approved people to access what they need during periods when an exception to the normal rules is needed but still having enough control that the organizations web usage policies are not compromised.

You are not restricted to having only one alternative profile as an option to the existing profile. The new profile depends on the credentials or IP address making the connection. For example, John connecting through the "Standard" profile could get the "Allow_Streaming_Video" profile while George would get the "Allow_Social_ Networking_Sites" profile.

The other thing to take into account is the time factor on these overrides. They are not indefinite. The longest that an override can be enabled is for 1 year less a minute. Often these overrides are set up for short periods of time for specific reasons such as a project. Having the time limitation means that the System Administrator does not have to remember to go back and turn the feature off after the project is finished.

Identity or Address

In either case what these override features do is, for specified users, user groups or IP addresses, allow sites blocked by Web Filtering profiles to be overridden for a specified length of time. The drawback of this method of override is that it takes more planning and preparation than the rating override method. The advantage is that once this has been set up, this method requires very little in the way of administrative overhead to maintain.

When planning to use the alternative profile approach keep in mind the following: In Boolean terms, one of the following "AND" conditions has to be met before overriding the Web Filter is possible

Based on the IP address:

- The Web Filter profile must be specified as allowing overrides
- AND the user's computer is one of the IP addresses specified
- AND the time is within the expiration time frame.

While the conditions are fewer for this situation there is less control over who has the ability to bypass the filtering configured for the site. All someone has to do is get on a computers that is allowed to override the Web Filter and they have access.

Based on user group:

- The Web Filter profile must be specified as allowing overrides
- AND the policy the traffic is going through must be identity based
- AND the user's credentials matches the identity credentials specified
- AND the time is within the expiration time frame.

This method is the one most likely to be used as it gives more control in that the user has to have the correct credential and more versatile because the user can use the feature from any computer that uses the correct policy to get out on the Internet.

Settings

When using an alternate profile approach to Web Filter overrides the following settings are used to determine authentication and outcome. Not every setting is used in both methods but enough of them are common to describe them collectively.

Apply to Group(s)

This is found in the Allow Blocked Overrides configuration. Individual users can not be selected. You can select one or more of the User Groups that are recognized my the FortiGate unit, whether they are local to the system or from a third part authentication device such as a AD server through FSSO.

Original Profile

This is found in the Administrative Override configuration. In the Allow Blocked Overrides setting the configuration is right inside the profile so there was no need to specify which profile was the original one, but the Administrative Override setup is done separately from the profiles themselves.

Assign to Profile or New Profile

Despite the difference in the name of the field, this is the same thing in both variations of the feature. You select from the drop down menu the alternate Web Filter Profile that you wish to set up for this override.

Scope or Scope Range

When setting up the override in the "Allow Blocked Overrides" variation you are given a drop down menu next to the field name Scope while in the Administrative Override configuration you are asked to select a radio button next to the same options. In both cases this is just a way of selecting which form of credentials will be required to approve the overriding of the existing Web Filter profile.

When the Web Filter Block Override message page appears it will display a field named "Scope:" and depending on the selection, it will show the type of credentials used to determine whether or not the override is allowed. The available options are:

- **User**
  This means that the authentication for permission to override will be based on whether or not the user is using a specific user account.

- **User Group**
  This means that the authentication for permission to override will be based on whether on not the user account supplied as a credential is a member of the specified User Group.

- **IP**
  This means that the authentication for permission to override will be based on the IP address of the computer that was used to authenticate. This would be used with computers that have multiple users. Example: If Paul logs on to the computer, engages the override using his credentials and then logs off, if the scope was based on the IP address of the computer, anybody logging in with any account on that computer would now be using the alternate override Web Filter profile.

  When entering an IP address in the Administrative Override version, only individual IP addresses are allowed.

  Differences between IP and Identity based scope

  - Using the IP scope does not require the use of an Identity based policy.
  - When using the Administrative Override variation and IP scope, you may not see a warning message when you change from using the original Web Filter profile to using the alternate profile. There is no requirement for credentials from the user so, if allowed, the page will just come up in the browser.
- **Ask**
  This option is available only in the "Allowed Blocked Overrides" variation and when used configures the message page to ask which scope the user wished to use. Normally, when the page appears the scope options are greyed out an not editable, but by using the ask option the option is dark and the user can choose from the choice of:
  - User
  - User Group
  - IP Address

- **Duration Mode**
  This option is available only in the "Allowed Blocked Overrides" variation. The Administrative Override sets a specified time frame that is always used for that override. The available options from the drop down menu are:
  - **Constant**
    Using this setting will mean that what ever is set as the duration will be the length of time that the override will be in effect. If the Duration variable is set to 15 minutes the length of the override will always be 15 minutes. The option will be visible in the Override message page but the setting will be greyed out.
  - **Ask**

    Using this setting will give the person the option of setting the duration to the override when it is engaged. The duration time which is greyed out if the Constant setting is used will be dark and editable. The user can set the duration in terms of Day, Hours and or Minutes.

- **Duration**
  Duration is on of the areas where the two variations takes a different approach, on two aspects of the setting. As already indicated the "Administrative Override" only uses a static time frame there is no option for the user to select on the fly how long it will last. The other way in which the two variation differ is that the "Allow Blocked Overrides" starts the clock when the user logs in with his credentials. For example, if the duration is 1 hour and John initiates an override at 2:00 p.m. on January 1, at the end of that hour he will revert back to using the original profile but he can go back and re-authenticate and and start the process over again. The Administrative override variation starts the clock from when the override was configured, which is why is shows an expiration date and time when your are configuring it.

  This option, which is available when the Duration Mode is set to Constant is the time in minutes that the override will last when engaged by the user.

  When setting up a constant duration in the Web Based Interface, minutes is the only option for units of time. To set a longer time frame or to use the units of hours or days you can use the CLI.

```
config webfilter profile
   edit <name of webfilter profile>
      config override
         set ovrd-dur <###d##h##m>
      end
```

When configuring the duration you don't have to set a value for a unit you are not using. If you are not using days or hours you can use:

```
set ovrd-dur 30m
```

instead of:

```
set ovrd-dur 0d0h30m
```

However, each of the units of time variable has their own maximum level:

```
###d cannot be more than 364
##h cannot be more than 23
##m cannot be more than 59
```

So the maximum length that the override duration can be set to is 364 days, 23 hours, and 59 minutes(a minute shy of 1 year) .

SafeSearch

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. For example, on a Google search it would mean adding the string “&safe=active” to the URL in the search.

The search sites supported are:

- Google
- Yahoo
- Bing
- Yandex

Enabling SafeSearch — CLI

```
config webfilter profile
   edit default
      config web
         set safe-search url
      end
   end
```

This enforces the use of SafeSearch in traffic controlled by the firewall policies using the web filter you configure.

Search Keywords

There is also the capability to log the search keywords used in the search engines.

YouTube Education Filter

YouTube for Schools is a way to access educational videos from inside a school network. This YouTube feature gives schools the ability to access a broad set of educational videos on YouTube EDU and to select the specific videos that are accessible from within the school network.

Before this feature can be used an account has to be set up for the school with YouTube. Once the account is set up a unique ID will be provided. This ID becomes part of the filter that is used to all access to the educational content of YouTube for use in schools even if YouTube is blocked by the policy.

More details can be found by going to http://www.youtube.com/schools.

Enabling YouTube Education Filter in CLI

```
config webfilter profile
   edit default
      config web
         set safe-search url header
         set youtube-edu-filter-id ABCD1234567890abcdef
      end
   end
```

Static URL Filter

You can allow or block access to specific URLs by adding them to the Web Site Filter list. You add the URLs by using patterns containing text and regular expressions. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to ftp:// ftp.example.com. Instead, use firewall policies to deny ftp connections.

When adding a URL to the URL filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls access to the news page on this web site.

- To control access to all pages with a URL that ends with example.com, add `example.com` to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.
- Control access to all URLs that match patterns using text and regular expressions (or wildcard characters). For example, `example.*` matches example.com, example.org, example.net and so on.

URLs with an action set to exempt or monitor are not scanned for viruses. If users on the network download files through the FortiGate unit from a trusted web site, add the URL of this web site to the URL filter list with an action to pass it so the FortiGate unit does not virus scan files downloaded from this URL.

URL formats

When adding a URL to the URL filter list, follow these rules:

How URL formats are detected when using HTTPS

If your unit does not support SSL content scanning and inspection or if you have selected the **URL filtering** option in web content profile for **HTTPS content filtering mode** under **Protocol Recognition**, filter HTTPS traffic by entering a top level domain name, for example, `www.example.com`. HTTPS URL filtering of encrypted sessions works by extracting the CN from the server certificate during the SSL negotiation. Since the CN only contains the domain name of the site being accessed, web filtering of encrypted HTTPS sessions can only filter by domain names.

If your unit supports SSL content scanning and inspection and if you have selected Deep Scan, you can filter HTTPS traffic in the same way as HTTP traffic.

How URL formats are detected when using HTTP

URLs with an action set to exempt are not scanned for viruses. If users on the network download files through the unit from trusted web site, add the URL of this web site to the URL filter list with an action set to exempt so the unit does not virus scan files downloaded from this URL.

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and filename to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls the news page on this web site.
- To control access to all pages with a URL that ends with `example.com`, add `example.com` to the filter list. For example, adding `example.com` controls access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.
- Control access to all URLs that match patterns created using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on.
- Fortinet URL filtering supports standard regular expressions.

If virtual domains are enabled on the unit, web filtering features are configured globally. To access these features, select **Global Configuration** on the main menu.

URL Filter actions

You can select one of four actions for how traffic will be treated as it attempts to reach a site in the list.

Block

Attempts to access any URLs matching the URL pattern are denied. The user will be presented with a replacement message.

Allow

Any attempt to access a URL that matches a URL pattern with an allow action is permitted. The traffic is passed to the remaining antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning.

Allow is the default action. If a URL does not appear in the URL list, it is permitted.

Monitor

Traffic to, and reply traffic from, sites matching a URL pattern with a monitor be allowed through in the same way as the “Allow” action. The difference with the Monitor action being that a log message will be generated each time a matching traffic session is established. The requests will also be subject to all other Security Profiles inspections that would normally be applied to the traffic.

Exempt

Exempt allows trusted traffic to bypass the antivirus proxy operations, but it functions slightly differently. In general, if you’re not certain that you need to use the **Exempt** action, use **Monitor**.

HTTP 1.1 connections are persistent unless declared otherwise. This means the connections will remain in place until closed or the connection times out. When a client loads a web page, the client opens a connection to the web server. If the client follows a link to another page on the same site before the connection times out, the same connection is used to request and receive the page data.

When you add a URL pattern to a URL filter list and apply the **Exempt** action, traffic sent to and replies traffic from sites matching the URL pattern will bypass all antivirus proxy operations. The connection itself inherits the exemption. This means that all subsequent reuse of the existing connection will also bypass all antivirus proxy operations. When the connection times out, the exemption is cancelled.

For example, consider a URL filter list that includes `example.com/files` configured with the Exempt action. A user opens a web browser and downloads a file from the URL `example.com/sample.zip`. This URL does not match the URL pattern so it is scanned for viruses. The user then downloads `example.com/files/beautiful.exe` and since this URL does match the pattern, the connection itself inherits the exempt action. The user then downloads `example.com/virus.zip`. Although this URL does not match the exempt URL pattern, a previously visited URL did, and since the connection inherited the exempt action and was re-used to download a file, the file is not scanned.

If the user next goes to an entirely different server, like `example.org/photos`, the connection to the current server cannot be reused. A new connection to example.org is established. This connection is not exempt. Unless the user goes back to example.com before the connection to that server times out, the server will close the connection. If the user returns after the connection is closed, a new connection to example.com is created and it is not exempt until the user visits a URL that matches the URL pattern.

Web servers typically have short time-out periods. A browser will download multiple components of a web page as quickly as possible by opening multiple connections. A web page that includes three photos will load more quickly if the browser opens four connections to the server and downloads the page and the three photos at the same time. A short time-out period on the connections will close the connections faster, allowing the server to avoid unnecessarily allocating resources for a long period. The HTTP session time-out is set by the server and will vary with the server software, version, and configuration.

Using the **Exempt** action can have unintended consequences in certain circumstances. You have a web site at example.com and since you control the site, you trust the contents and configure `example.com` as exempt. But example.com is hosted on a shared server with a dozen other different sites, each with a unique domain name. Because of the shared hosting, they also share the same IP address. If you visit example.com, your connection your site becomes exempt from any antivirus proxy operations. Visits to any of the 12 other sites on the same server will reuse the same connection and the data you receive is exempt from scanned.

Use of the **Exempt** action is not suitable for configuration in which connections through the FortiGate unit use an external proxy. For example, you use proxy.example.net for all outgoing web access. Also, as in the first example, URL filter list that includes a URL pattern of `example.com/files` configured with the **Exempt** action. Users are protected by the antivirus protection of the FortiGate unit until a user visits a URL that matches the of `example.com/files` URL pattern. The pattern is configured with the **Exempt** action so the connection to the server inherits the exemption. With a proxy however, the connection is from the user to the proxy. Therefore, the user is entirely unprotected until the connection times out, no matter what site he visits.

Ensure you are aware of the network topology involving any URLs to which you apply the Exempt action.

Status

The Web Site Filter has the option to either enable or disable individual web sites in the list. This allows for the temporary removal of the actions against a site so that it can be later reengaged without having to rewrite the configuration.

Configuring a URL filter

Each URL filter list can have up to 5000 entries. For this example, the URL www.example*.com will be used. You configure the list by adding one or more URLs to it.

To add a URL to a URL filter

1. Go to **Security Profiles > Web Filter**
2. Select a web filter to edit.
3. In the URL filter, select **Create New**.
4. Enter the URL, without the “http”, for example: `www.example*.com`.
5. Select a **Type**: **Simple** (see below), **Wildcard**, or **Regular Expression**.
6. In this example, select **Wildcard**.
7. Select the **Action** to take against matching URLs: Exempt, Block, Allow, or Monitor.
8. Select **Enable**.
9. Select **OK.**

'Simple' filter type

If you select the **Simple** filter type for a URL filter, the syntax is performing an exact match. Note, however, that the domain and path are separate entities in HTTP despite the fact that a user types them as a single entity and, in the case of 'simple', the rules for each part (domain and path) are different.

The 'domain' part

For the domain part, the goal of the 'simple' format is to make it easy to block a domain and all its subdomains, such that the admin only has to type “address.xy" to block "address.xy", "www.address.xy", "talk.address.xy", etc. but *not* block “youraddress.xy" or "www.youraddress.xy" which are different domains from "address.xy”.

Also, the actual domain does not include http:// or https:// so this should *not* be entered or the URL filter will try to match a domain starting with http. For this reason, when you enter http:// in the URL filter via the GUI, it is automatically removed.

A trailing ‘/‘ with the domain is not needed. The GUI URL filter will automatically trim this, but when using the API to provide the per-user BWL it will not!

Please take this into account. Better not to use it as it might give unexpected results.

The 'path' part

For the path part, an exact match takes place. For example:

www.address.xy/news

blocks anything that starts with that exact path. So this matches:

www.address.xy/newsies
www.address.xy/newsforyou
www.address.xy/news/co
etc.

Also:

www.address.xy/new

likewise blocks the same as above but includes:

/newt
/newp
etc.

which is a much broader filter, matching:

www.address.xy/newstand/co
www.address.xy/news/co
etc.

In other words, the more you specify of the path, the more strictly it will match.

Here as well a trailing ‘/‘ with the URL path is not needed, the GUI URL filter will automatically trim this, but when using the API to provide the per-user BWL it will not!

Please take this into account. Better not to use it as it might give unexpected results.

Referer URL

A new variable has been added to the Static URL Filter, `referrer-host`. If a referer is specified, the hostname in the referer field of the HTTP require will be compared for any entry that contains the matching URL. If the referer matches, then the specified action will be performed by proxy.

Configuring in the GUI

The configuration can be done in the GUI but only if advance webfiltering features have been enabled by entering the following commands in the CLI:

```
config system global
   set gui-webfilter-advanced enable
end
```

After this command is used, a new column will be created in **Security Profiles > Web Filter > Static URL Filter** to set the referer.

Configuring in the CLI

When specifying the URL filter, it needs to be identified by its ID. The URLs are listed under each entry.

To find the ID number:

```
config webfilter urlfilter
   edit ?
```

A list of the current URL filters will be listed with their ID numbers in the left column.

The syntax in the CLI for configuring an entry is:

```
config webfilter urlfilter
   edit <ID>
      config entries
         edit 1
            set url <url>
            set referrer-host <url>
            set type {simple | regex | wildcard}
            set action {block | allow | monitor | exempt}
            set status {enable | disable}
         end
      end
   end
```

Web content filter

You can control web content by blocking access to web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can also add words, phrases, patterns, wild cards and Perl regular expressions to match content on web pages. You can add multiple web content filter lists and then select the best web content filter list for each web filter profile.

Enabling web content filtering involves three separate parts of the FortiGate configuration.

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day.

- The web filter profile specifies what sort of web filtering is applied.
- The web content filter list contains blocked and exempt patterns.

The web content filter feature scans the content of every web page that is accepted by a security policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than a threshold set in the web filter profile, the FortiGate unit blocks the page.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a web content filter list.
2. Add patterns of words, phrases, wildcards, and regular expressions that match the content to be blocked or exempted.
3. You can add the patterns in any order to the list. You need to add at least one pattern that blocks content.
4. In a web filter profile, enable the web content filter and select a web content filter list from the options list.

To complete the configuration, you need to select a security policy or create a new one. Then, in the security policy, enable **Webfilter** and select the appropriate web filter profile from the list.

Creating a web filter content list

You can create multiple content lists and then select the best one for each web filter profile. Creating your own web content lists can be accomplished only using the CLI.

This example shows how to create a web content list called inappropriate language, with two entries, offensive and rude.

To create a web filter content list

```
config webfilter content
   edit 3
      set name "inappropriate language"
      config entries
         edit offensive
            set action block
            set lang western
            set pattern-type wildcard
            set score 15
            set status enable
         next
         edit rude
            set action block
            set lang western
            set pattern-type wildcard
            set score 5
            set status enable
         end
      end
   end
```

Configuring a web content filter list

Once you have created the web filter content list, you need to add web content patterns to it. There are two types of patterns: **Wildcard** and **Regular Expression**.

You use the **Wildcard** setting to block or exempt one word or text strings of up to 80 characters. You can also use the wildcard symbols, such as “*” or “?”, to represent one or more characters. For example, as a wildcard expression, forti*.com will match fortinet.com and forticare.com. The “*” represents any kind of character appearing any number of times.

You use the **Regular Expression** setting to block or exempt patterns of Perl expressions, which use some of the same symbols as wildcard expressions, but for different purposes. The “*” represents the character before the symbol. For example, forti*.com will match fortiii.com but not fortinet.com or fortiice.com. The symbol “*” represents “i” in this case, appearing any number of times. RP: Add a regex example.

The maximum number of web content patterns in a list is 5000.

How content is evaluated

Every time the web content filter detects banned content on a web page, it adds the score for that content to the sum of scores for that web page. You set this score when you create a new pattern to block the content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the sum of scores equals or exceeds the threshold score, the web page is blocked. The default score for web content filter is 10 and the default threshold is 10. This means that by default a web page is blocked by a single match. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

Banned words or phrases are evaluated according to the following rules:

- The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.
- The score for any word in a phrase without quotation marks is counted.
- The score for a phrase in quotation marks is counted only if it appears exactly as written.

The following table describes how these rules are applied to the contents of a web page. Consider the following, a web page that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.”

Banned Pattern Rules

Banned pattern	Assigned score	Score added to the sum for the entire page	Threshold score	Comment
word	20	20	20	Appears twice but only counted once. Web page is blocked.
word phrase	20	40	20	Each word appears twice but only counted once giving a total score of 40. Web page is blocked
word sentence	20	20	20	“word” appears twice, “sentence” does not appear, but since any word in a phrase without quotation marks is counted, the score for this pattern is 20. Web page is blocked.
“word sentence”	20	0	20	“This phrase does not appear exactly as written. Web page is allowed.
“word or phrase”	20	20	20	This phrase appears twice but is counted only once. Web page is blocked.

Enabling the web content filter and setting the content threshold

When you enable the web content filter, the web filter will block any web pages when the sum of scores for banned content on that page exceeds the content block threshold. The threshold will be disregarded for any exemptions within the web filter list.

Advanced web filter configurations

Allow websites when a rating error occurs

Enable to allow access to web pages that return a rating error from the FortiGuard Web Filter service.

If your FortiGate unit cannot contact the FortiGuard service temporarily, this setting determines what access the FortiGate unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.

ActiveX filter

Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX may not function properly with this filter enabled.

Block HTTP redirects by rating

Enable to block HTTP redirects.

Many web sites use HTTP redirects legitimately but in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.

This option is not supported for HTTPS.

Block Invalid URLs

Select to block web sites when their SSL certificate CN field does not contain a valid domain name.

FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is not selected, the following behavior occurs:

- If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name.
- If the request is to a web server proxy, the real IP address of the web server is not known. Therefore, rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.

Enabling the Web Filter profile to block a particular category and enabling the Application Control profile will not result in blocking the URL. This occurs because Proxy and Flow based profiles cannot operate together.

To ensure replacement messages show up for blocked URLs, switch the Web Filter to Flow based inspection.

Cookie filter

Enable to filter cookies from web traffic. Web sites using cookies may not function properly with this enabled.

Provide Details for Blocked HTTP 4xx and 5xx Errors

Enable to have the FortiGate unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.

HTTP POST action

Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.

The available actions include:

Comfort

Use client comforting to slowly send data to the web server as the FortiGate unit scans the file. Use this option to prevent a server time-out when scanning or other filtering is enabled for outgoing traffic.

The client comforting settings used are those defined in the Proxy Options profile selected in the security policy.

Block

Block the HTTP POST command. This will limit users from sending information and files to web sites.

When the post request is blocked, the FortiGate unit sends the http-post-block replacement message to the web browser attempting to use the command.

Java applet filter

Enable to filter java applets from web traffic. Web sites using java applets may not function properly with this filter enabled.

Rate Images by URL

Enable to have the FortiGate retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category.

Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.

Rate URLs by Domain and IP Address

Enable to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter.

If the rating determined by the domain name and the rating determined by the IP address defer the Action that is enforce will be determined by a weighting assigned to the different categories. The higher weighted category will take precedence in determining the action. This will have the side effect that sometimes the Action will be determined by the classification based on the domain name and other times it will be determined by the classification that is based on the IP address.

FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to allow access to sites that should be blocked, or to block sites that should be allowed.

An example of how this would work would be if a URL's rating based on the domain name indicated that it belonged in the category Lingerie and Swimsuit, which is allowed but the category assigned to the IP address was Pornography which has an action of Block, because the Pornography category has a higher weight the effective action is Block.

Web resume download block

Enable to prevent the resumption of a file download where it was previously interrupted. With this filter enabled, any attempt to restart an aborted download will download the file from the beginning rather than resuming from where it left off.

This prevents the unintentional download of viruses hidden in fragmented files.

Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may also break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.

Restrict Google account usage to specific domains

This feature allows the blocking of access to some Google accounts and services while allowing access to accounts that are included in the domains specified in the exception list.

Block non-English character URLs

The FortiGate will not successfully block non-English character URLs if they are added to the URL filter. In order to block access to URLs with non-English characters, the characters must be translated into their international characters.

Browse to the non-English character URL (for example, http://www.fortinet.com/pages/ที่ นี่ -ไม่ มี เศษรั ฐประหารให้ ใครแดก/338419686287505?ref=stream).

On the FortiGate, use the URL shown in the FortiGate GUI and add it the list of blocked URLs in your URL filter (for example, http://www.fortinet.com/pages/%E0%B8%97%E0%B8%B5%E0%B9%88%E0%B8%99%E0%B8%B5%E0%B9%88-%E0%B9%84%E0%B8%A1%E0%B9%88%E0%B8%A1%E0%B8%B5%E0%B9%80%E0%B8%A8%E0%B8%A9%E0%B8%A3%E0%B8%B1%E0%B8%90%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%AB%E0%B8%B2%E0%B8%A3%E0%B9%83%E0%B8%AB%E0%B9%89%E0%B9%83%E0%B8%84%E0%B8%A3%E0%B9%81%E0%B8%94%E0%B8%81/338419686287505?ref=stream).

Once added, further browsing to the URL will result in a blocked page.

CLI Syntax

```
config webfilter urlfilter
   edit 1
      set name "block_international_character_urls"
         config entries
            edit 1
               set url "www.fortinet.com/pages/2.710850E-3120%B8%E0%B8%B53.231533E-
                   3170%B9%E0%B8%E0%B8%B53.231533E-3170%B9%88-3.230415E-
                   3170%B9%E0%B80X0.000000063CD94P-102211.482197E-
                   3230%B9%E0%B80X0.0007FBFFFFCFP-102210.000000E+000%B8%B51.828043E-
                   3210%B9%E0%B80X0P+081.828043E-3210%B80X0P+092.710850E-
                   3120%B80X0.0000000407ED2P-102233.236834E-3170%B8%B19.036536E-
                   3130%B8%E0%B8%9B4.247222E-3140%B80X0P+039.036683E-3130%B8%B02.121996E-
                   3130%B80X0.0000000000008P-1022B2.710850E-3120%B8%B21.482197E-
                   3230%B80X0P+030.000000E+000%B9%E0%B80X0P+0B2.710850E-
                   3120%B9%E0%B9%E0%B8%E0%B80X0.0000000408355P-102232.023693E-
                   3200%B9%E0%B8%E0%B8%81/338419686287505?ref=stream"
               set action block
            next
         end
   next
end

config webfilter urlfilter
   edit 2
      set name "block_international_character_urls"
   next
end

config webfilter profile
   edit "block_international_character_urls"
   next
end

config firewall policy
   edit 3
      set uuid cf80d386-7bcf-51e5-6e87-db207e3f0fa8
```

```
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set webfilter-profile "block_international_character_urls"
        set profile-protocol-options "default"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
    next
end
```

Configuring Web Filter Profiles

Enabling FortiGuard Web Filter

FortiGuard Web Filter is enabled and configured within web filter profiles by enabling FortiGuard Categories. The service is engaged by turning on the Web Filter profile and selecting a profile that has FortiGuard Categories enabled on one or more active policies being run by the firewall.

There is also a system wide setting for the enabling or disabling of FortiGuard Web Filter that is only in the CLI.

```
config system fortiguard
   set webfilter-force-off
```

The two options on this setting are enable or disable. The syntax of the settings name is “force-off” so in order to enable FortiGuard Webfilter you have to choose disable for the setting and enable if you want to turn it off.

General configuration steps

1. Go to **Security Profiles > Web Filter**.
2. Determine if you wish to create a new profile or edit an existing one.
3. Select an **Inspection Mode**.
4. If you are using FortiGuard Categories, enable the FortiGuard Categories, select the categories and select the action to be performed.
5. Configure any **Quotas** needed. (Proxy Mode)
6. Allow blocked override if required.(Proxy Mode)
7. Set up **Safe Search** settings and/or YouTube Education settings. (Proxy & Flow-based)
8. Configure **Static URL Settings**. (All Modes)
9. Configure **Rating Options**. (All Modes)
10. Configure **Proxy Options**.
11. Save the filter and web filter profile.
12. To complete the configuration, you need to select the security policy controlling the network traffic you want to restrict. Then, in the security policy, enable Web Filter and select the appropriate web filter profile from the list.

Configuring FortiGuard Web Filter settings

FortiGuard Web Filter includes a number of settings that allow you to determine various aspects of the filtering behavior.

Getting to the Edit Web Filter Profile configuration window

Once you have gotten to the profile configuration window there are a number of settings that can be used, most of which are optional. We will treat each of these options separately, but present the common instructions of how to get to the profile editing page here.

1. Go to **Security Profiles > Web Filter**.
2. Determine if you wish to create a new profile, edit an existing one, or clone and then edit an existing one.
   a. New profile:
      i. Select the **Create New** icon, in the upper right of the window (looks like a plus sign in a circle) **OR**
      ii. Select the **List** icon, in the upper right (looks like a white rectangle with lines like text). Select the **Create New** icon in the upper left.
   b. Edit existing profile:
      i. Select the name of the profile that you wish to edit from the drop-down menu **OR**
      ii. Select the **List** icon, in the upper right (looks like a white rectangle with lines like text. Highlight the name of the profile from the list and select **Edit** from the options above the list.
   c. Clone a profile:
      i. Select **Clone** icon in the upper right corner of the window (looks like one sheet of lined paper overlapping another) **OR**
      ii. Select the **List**icon, in the upper right (looks like a white rectangle with lines like text. Highlight the name of the profile from the list and select **Clone** from the options above the list.
3. Make sure there is a valid name, and comment if you want.
4. Configure the settings to best achieve your specific requirements
5. Select **Apply** or **OK, depending on whether you are editing or creating a new profile.**.

In older versions of FortiOS there was a character limitation for the URL of 2048 bytes or approximately 321 characters. If the URL you were trying to reach was longer the URL sent to FortiGuard would be truncated and the service would be unable to categorize the site. Starting in version 5 of the firmware the parsed URL has been increase to 4 Kilobytes, effectively doubling the length of a URL capable of being categorized.

To configure the FortiGuard Web Filter categories

1. Go to the **Edit Web Filter Profile** window.
2. The category groups are listed in a widget. You can expand each category group to view and configure every sub-category individually within the groups. If you change the setting of a category group, all categories within the group inherit the change.
3. Select the category groups and categories to which you want to apply an action.
   To assign an action to a category left click on the category and select from the pop up menu.
4. Enable **Enforce Quota** to activate the quota for the selected categories and category groups.

5. Select **Hours**, **Minutes**, or **Seconds** and enter the number of hours, minutes, or seconds. This is the daily quota allowance for each user.
6. Select **Apply** or **OK**.

Apply the web filter profile to an identity-based security policy. All the users subject to that policy are restricted by the quotas.

If you look at your logs carefully, you may notice that not every URL connection in the log shows a category. They are left blank. If you take one of those URL and enter it in the FortiGuard website designed to show the category for a URL it will successfully categorize it.

The reason for this is that to optimize speed throughput and reduce the load on the FortiGuard servers the FortiGate does not determine a category rating on scripts and css files.

Configuring FortiGuard Category Quotas

1. Go to the Edit Web Filter Profile window
2. Verify that the categories that need to have quotas on them are set to one of the actions:
   - Monitor
   - Warning
   - Authenticate
3. Select the blue triange expand symbol to show the widget for Quotas
4. Select **Create New** or **Edit**.
5. In the **New/Edit Quota** window that pops up enable or disable the specific categories that the quota will apply to.
6. At the bottom of the widget, select **Hours**, **Minutes**, or **Seconds** and enter the number of hours, minutes, or seconds. This is the daily quota allowance for each user.
7. Select **Apply or OK**.
8. Continue with any other configuration in the profile
9. Select **Apply or OK**.

Apply the web filter profile to an identity-based security policy. All the users subject to that policy are restricted by the quotas.

Timed access quota can be configured through the GUI. You can also use CLI commands to configure a bandwidth quota. The following commands show how to add a quota of 10MB of bandwidth. Refer to the FortiOS 5.2 CLI Reference Guide for more information.

```
config webfilter profile
   edit default
      config ftgd-wf
         config quota
            edit <id>
               set category <id>
               set type traffic
               set unit MB
               set value 10
            end
         end
      end
```

Configure Allowed Blocked Overrides

1. Go to the **Edit Web Filter Profile window.**
2. Enable **Allow Blocked Override**
3. In the Apply to Group(s) field select the desired **User Group**
4. In the Assign to Profile field, select the desired profile

Configure Search Engine Section

There are 2 primary configuration settings in this section.

Enable Safe Search

To enable the Safe Search settings

1. Go to the **Edit Web Filter Profile window.**
2. Enable **Safe Search**
3. Enable Search Engine Safe Search
4. Enable YouTube Filter
   a. Enter the YouTube User ID in the Text field

Log All Search Keywords

In the GUI, the configuration setting is limited to a checkbox.

Configure Static URL Filter

Web Content Filter

To enable the web content filter and set the content block threshold

1. Go to the **Edit Web Filter Profile window**.
2. In the **Static URL Filter section** enable **Web Content Filter**.
3. Select **Create New**.
4. Select the **Pattern Type**.
5. Enter the content **Pattern**.
6. Enter the **Language** from the dropdown menu.
7. Select **Block** or **Exempt**, as required, from the **Action** list.
8. Select **Enable**.
9. Select **OK.**

Configure Rating Options

Allow Websites When a Rating error Occurs

In the GUI, the configuration setting is limited to a checkbox.

Rate URLs by Domain and IP Address

In the GUI, the configuration setting is limited to a checkbox.

Block HTTP Redirects by Rating

In the GUI, the configuration setting is limited to a checkbox.

Rate Images by URL (Blocked images will be replaced with blanks)

In the GUI, the configuration setting is limited to a checkbox.

Configure Proxy Options

Restrict Google Account Usage to Specific Domains

Configuring the feature in the GIU

Go to **Security Profiles > Web Filter**.

In the **Proxy Options** section, check the box next to **Restrict to Corporate Google Accounts Only**.

Use the **Create New** link within the widget to add the appropriate Google domains that will be allowed.

Configuring the feature in the CLI

To configure this option in the CLI, the URL filter must refer to a web-proxy profile that is using the Modifying HTTP Request Headers feature. The command is only visible when the action for the entry in the URL filter is set to either allow or monitor.

1. Configure the proxy options:

```
config web-proxy profile
   edit "googleproxy"
      config headers
         edit 1
            set name "X-GoogApps-Allowed-Domains"
            set content "fortinet.com, Ladan.ca"
            end
         end
      end
   end
```

2. Set a web filter profile to use the proxy options

```
config webfilter urlfilter
   edit 1
      config entries
         edit "*.google.com"
            set type wildcard
            set action {allow | monitor}
            set web-proxy-profile <profile>
            end
         end
      end
   end
```

In the CLI, you can also add, modify, and remove header fields in HTTP request when scanning web traffic in proxy-mode. If a header field exists when your FortiGate receives the request, its content will be modified based on the configurations in the URL filter.

Web Resume Download block

In the GUI, the configuration setting is limited to a checkbox.

Provide Details for Blocked HTTP 4xx and 5xx Errors

In the GUI, the configuration setting is limited to a checkbox.

HTTP POST Action

Remove Java Applet Filter

In the GUI, the configuration setting is limited to a checkbox.

Remove ActiveX Filter

In the GUI, the configuration setting is limited to a checkbox.

Remove Cookie Filter

In the GUI, the configuration setting is limited to a checkbox.

Web filtering example

Web filtering is particularly important for protecting school-aged children. There are legal issues associated with improper web filtering as well as a moral responsibility not to allow children to view inappropriate material. The key is to design a web filtering system in such a way that students and staff do not fall under the same web filter profile in the FortiGate configuration. This is important because the staff may need to access websites that are off-limits to the students.

School district

The background for this scenario is a school district with more than 2300 students and 500 faculty and staff in a preschool, three elementary schools, a middle school, a high school, and a continuing education center. Each elementary school has a computer lab and the high school has three computer labs with connections to the Internet. Such easy access to the Internet ensures that every student touches a computer every day.

With such a diverse group of Internet users, it was not possible for the school district to set different Internet access levels. This meant that faculty and staff were unable to view websites that the school district had blocked. Another issue was the students' use of proxy sites to circumvent the previous web filtering system. A proxy server acts as a go-between for users seeking to view web pages from another server. If the proxy server has not been blocked by the school district, the students can access the blocked website.

When determining what websites are appropriate for each school, the district examined a number of factors, such as community standards and different needs of each school based on the age of the students.

The district decided to configure the FortiGate web filtering options to block content of an inappropriate nature and to allow each individual school to modify the options to suit the age of the students. This way, each individual

school was able to add or remove blocked sites almost immediately and have greater control over their students' Internet usage.

In this simplified example of the scenario, the district wants to block any websites with the word **example** on them, as well as the website www.example.com. The first task is to create web content filter lists for the students and the teachers.

Create a Webfilter for the students

1. Go to **Security Profiles** > **Web Filter.**
2. Select the Create New icon.
3. Enter the name "Students" in the name field.
4. For the Inspection mode, select Proxy.
5. Enable FortiGuard Categories.
   a. Set to block the following categories:
   - Potentially Liable
   - Adult/Mature Content
   - Security Risk

URL Content

6. Check Enable Safe Search
   a. Check **Search Engine Safe Search - Google, Yahoo!, Bing, Yandex**
   b. Check **YouTube Education Filter** and enter the YouTube User ID
7. In the Static URL Filter section, check Enable URL Filter.
   a. In the URL Filter widget, Select **Create New**.
      i. In the **URL** field, enter *example*.*
      ii. For the **Type** field, select Wildcard
      iii. For the **Action** field, select Block
      iv. For the **Status** field, check enable
      v. Select **OK**

Web Content Filter

8. In the Static URL Filter section, check Enable Web Content Filter.
   a. In the Web Content Filter widget, select **Create New**.
   b. Enter the name "Teachers" in the name field.
      i. For the **Pattern Type** field, select
      ii. In the **Pattern** field, enter "example"
      iii. For the **Language** field, choose Western
      iv. For the **Action** field, select "Block"
      v. For the **Status** field, check Enable.
      vi. Select **OK**
9. Check **Rate URLs by Domain and IP Address**
10. Check Block HTTP Redirects by Rating

11. Check **Rate Images by URL (Blocked images will be replaced with blanks)**
12. Select **OK**

Create a Webfilter for the Teachers

It might be more efficient if the Teacher Web Content List included the same blocked content as the student list. From time to time a teacher might have to view a blocked page. It would then be a matter of changing the **Action** from **Block** to **Allow** as the situation required. The following filter is how it could be set up for the teachers to allow them to see the “example” content if needed while keeping the blocking inappropriate material condition.

1. Go to **Security Profiles** > **Web Filter.**
2. Select the Create New icon.
3. Enter the name “Teachers” in the name field.
4. For the Inspection mode, select Proxy.
5. Enable FortiGuard Categories.
   a. Set to block the following categories:
   - Potentially Liable
   - Adult/Mature Content
   - Security Risk

URL Content

6. Check Enable Safe Search
   a. Check **Search Engine Safe Search - Google, Yahoo!, Bing, Yandex**
   b. Check **YouTube Education Filter** and enter the YouTube User ID
7. In the Static URL Filter section, check Enable URL Filter.
   a. In the URL Filter widget, Select **Create New**.
      i. In the **URL** field, enter *example*.*
      ii. For the **Type** field, select Wildcard
      iii. For the **Action** field, select Block
      iv. For the **Status** field, check enable
      v. Select **OK**

Web Content Filter

8. In the Static URL Filter section, check Enable Web Content Filter.
   a. In the Web Content Filter widget, select **Create New**.
   b. Enter the name “Teachers” in the name field.
      i. For the **Pattern Type** field, select
      ii. In the **Pattern** field, enter “example”
      iii. For the **Language** field, choose Western
      iv. For the **Action** field, select “Exempt”
      v. For the **Status** field, check Enable.
      vi. Select **OK**
9. Check **Rate URLs by Domain and IP Address**
10. Check Block HTTP Redirects by Rating

11. Check **Rate Images by URL (Blocked images will be replaced with blanks)**
12. Select **OK**

To create a security policy for the students

1. Go to **Policy > Policy > IPv4.**
2. Select the policy being used to manage student traffic.
3. Enable **Web Filter**.
4. Select **Students** from the web filter drop-down list.
5. Select **OK**.

To create a security policy for Teachers

1. Go to **Policy > Policy > IPv4.**
2. Select the policy being used to manage teacher traffic.
3. Enable **Web Filter**.
4. Select **Teachers** from the web filter drop-down list.
5. Select **OK**.
6. Make sure that the student policy is in the sequence before the teachers' policy.

Application control

Using the application control Security Profile feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

Fortinet is constantly increasing the list of applications that application control can detect by adding applications to the FortiGuard Application Control Database. Because intrusion protection protocol decoders are used for application control, the application control database is part of the FortiGuard Intrusion Protection System Database and both of these databases have the same version number.

You can find the version of the application control database that is installed on your unit, by going to the **License Information** dashboard widget and find IPS Definitions version.

You can go to the FortiGuard Application Control List to see the complete list of applications supported by FortiGuard. This web page lists all of the supported applications. You can select any application name to see details about the application.

If you enable virtual domains (VDOMs) on the Fortinet unit, you need to configure application control separately for each virtual domain.

The following topics are included in this section:

- Application control concepts
- Application considerations
- Application traffic shaping
- Application control monitor
- Enable application control
- Application control examples

To view the version of the application control database installed on your FortiGate unit, go to the **License Information** dashboard widget and find the **IPS Definitions** version.

To see the complete list of applications supported by FortiGuard Application Control go to the FortiGuard Application Control List. This web page lists all of the supported applications. You can select any application name to see details about the application.

Application control concepts

You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the

application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.

Updated and new application signatures are delivered to your FortiGate unit as part of your FortiGuard Application Control Service subscription. Fortinet is constantly increasing the number of applications that application control can detect by adding applications to the FortiGuard Application Control Database. Because intrusion protection protocol decoders are used for application control, the application control database is part of the FortiGuard Intrusion Protection System Database and both of these databases have the same version number.

To view the version of the application control database installed on your FortiGate unit, go to the **License Information** dashboard widget and find the **IPS Definitions** version.

To see the complete list of applications supported by FortiGuard Application Control go to the FortiGuard Application Control List. This web page lists all of the supported applications. You can select any application name to see details about the application.

Application Control Actions

Allow

This action allows the targeted traffic to continue on through the FortiGate unit.

Monitor

This action allows the targeted traffic to continue on through the FortiGate unit but logs the traffic for analysis.

Block

This action prevents all traffic from reaching the application and logs all occurrences.

Reset

This action resets the session or connection between the FortiGate and the initiating node.

Traffic Shaping

This action presents a number of default traffic shaping options:

- guarantee-100kbps
- high-priority
- low-priority
- medium-priority
- shared-1M-pipe

View Signatures

This option brings up a window that displays a list of the signatures with the following columns:

- Application Name
- Category

- Technology - Technology is broken down into 3 technology models as well as the more basic Network-Protocol which would can be used as a catch all for anything not covered by the more narrowly defined technologies of:
  - Browser-Based
  - Client-Server
  - Peer -to-Peer
- Popularity - Popularity is broken down into 5 levels of popularity represented by stars. 5 stars representing the most popular applications and 1 star representing applications that are the least popular.
- Risk - The Risk property does not indicate the level of risk but the type of impact that is likely to occur by allowing the traffic from that application to occur. The Risk list is broken down into the following

Application considerations

Some applications behave differently from most others. You should be aware of these differences before using application control to regulate their use.

IM applications

The Application Control function for a number of IM application is not in the Web Based Manager, in the CLI of the FortiGate unit. These applications are:

- AIM
- ICQ
- MSN
- Yahoo

These applications are controlled by either permitting or denying the users from logging in to the service. Individual IM accounts are configured as to whether or not they are permitted and then there is a global policy for how to action unknown users, by the application, and whether to add the user to the black list or the white list.

The configuration details for these settings can be found in the CLI Reference guide under the heading of imp2p.

Skype

Based on the NAT firewall type, Skype takes advantage of several NAT firewall traversal methods, such as STUN (Simple Traversal of UDP through NAT), ICE (Interactive Connectivity Establishment) and TURN (Traversal Using Relay NAT), to make the connection.

The Skype client may try to log in with either UDP or TCP, on different ports, especially well-known service ports, such as HTTP (80) and HTTPS (443), because these ports are normally allowed in firewall settings. A client who has previously logged in successfully could start with the known good approach, then fall back on another approach if the known one fails.

The Skype client could also employ Connection Relay. This means if a reachable host is already connected to the Skype network, other clients can connect through this host. This makes any connected host not only a client but also a relay server.

SPDY

SPDY (pronounced speedy, it's a trademarked name not an acronym) is a networking protocol developed to increase the speed and security of HTML traffic. It was developed primarily by Google. The Application Control engine recognises this protocol and its required SSL/TLS component within Application Control sensors. It is counted as part of application traffic for Google and other sources that use the protocol.

Working with other FortiOS components

Application Control is not just a modulal that is inserted in to the OS and works independantly of all of the other components.

WAN Optimization

There is a feature that enables both IPS and Application Control on both non-HTTP WANOpt traffic and HTTP-tunneled traffic through HTTP CONNECT. The basic idea is that it hooks a scan connection to a port so that traffic will be redirected to the IPS engine before forwarding to a different module.

Application traffic shaping

You can apply traffic shaping for application list entries you configure to pass. Traffic shaping enables you to limit or guarantee the bandwidth available to the application or applications specified in an application list entry. You can also prioritize traffic by using traffic shaping.

You can create or edit traffic shapers by going to **Policy & Objects > Objects > Traffic Shapers**.

Direction of traffic shaping

When Traffic Shaping is enabled the direction that traffic shaping will be applied must also be chosen.

Forward direction traffic shaping refers to the direction of the initial connection. This would be the direction described by the policy that the Application Control Sensor is assigned to. If the policy has an Incoming Interface of LAN and an Outgoing Interface of wan1 then any Forward Direction Traffic Shaping profile will apply to network traffic heading in that direction only. If the connection used by that policy involved a response that included a download of Gigabytes of traffic the shaper would not be applied to that traffic.

Reverse Direction Traffic Shaping is applied to traffic that is flowing in the opposite direction indicated by the direction of the policy. If the policy has an Incoming Interface of LAN and an Outgoing Interface of wan1 then the shaper would only be applied to the traffic that was coming from the wan1 interface to the LAN interface.

For example, if you find that your network bandwidth is being overwhelmed by streaming HTTP video, one solution is to limit the bandwidth by applying a traffic shaper to an application control entry that allows the HTTP.Video application. Your users access the Web using a security policy that allows HTTP traffic from the internal interface to the external interface. Firewall policies are required to initiate communication so even though web sites respond to requests, a policy to allow traffic from the external interface to the internal interface is not required for your users to access the Web. The internal to external policy allows them to open communication sessions to web servers, and the external servers can reply using the existing session.

If you enable **Traffic Shaping** and select the Forward Direction shaper in an application sensor specified in the security policy, the problem will continue. The reason is the shaper you select for **Traffic Shaping** is applied only to the application traffic moving in the direction stated in the security policy. In this case, that is from the internal interface to the external interface. The security policy allows the user to visit the web site and start the video, but the video itself is streamed from the server to the user, or from the external interface to the internal interface. This is the reverse of the direction specified in the security policy. To solve the problem, you must enable **Reverse Direction Traffic Shaping** and select the appropriate shaper.

Shaper re-use

Shapers are created independently of firewall policies and application sensors so you are free to reuse the same shapers in multiple list entries and policies. Shared shapers can be configured to apply separately to each security

policy or across all policies. This means that if a shaper is configured to guaranteed 1000 KB/s bandwidth, each security policy using the shaper will have its own 1000 KB/s reserved, or all of the policies using the shaper will share a pool if 1000 KB/s, depending on how it is configured.

The same thing happens when a shaper is used in application sensors. If an application sensor using a shaper is applied to two separate policies, how the bandwidth is limited or guaranteed depends on whether the shaper is set to apply separately to each policy or across all policies. In fact, if a shaper is applied directly to one security policy, and it is also included in an application sensor that is applied to another security policy, the same issue occurs. How the bandwidth is limited or guaranteed depends on the shaper configuration.

If a shaper is used more than once within a single application sensor, all of the applications using the shaper are restricted to the maximum bandwidth or share the same guaranteed bandwidth.

For example, you want to limit the bandwidth used by Skype and Facebook chat to no more than 100 KB/s. Create a shaper, enable **Maximum Bandwidth**, and enter 100. Then create an application sensor with an entry for Skype and another entry for Facebook chat. Apply the shaper to each entry and select the application sensor in the security policy that allows your users to access both services.

This configuration uses the same shaper for each entry, so Skype **and** Facebook chat traffic are limited to no more than 100 KB/s in total. That is, traffic from both applications is added and the total is limited to 100 KB/s. If you want to limit Skype traffic to 100 KB/s and Facebook chat traffic to 100 KB/s, you must use separate shapers for each application control entry.

Application control monitor

The application monitor enables you to gain an insight into the applications generating traffic on your network. When monitor is enabled in an application sensor entry and the list is selected in a security policy, all the detected traffic required to populate the selected charts is logged to the SQL database on the FortiGate unit hard drive. The charts are available for display in the executive summary section of the log and report menu.

Because the application monitor relies on a SQL database, the feature is available only on FortiGate units with an internal hard drive.

While the monitor charts are similar to the top application usage dashboard widget, it offers several advantages. The widget data is stored in memory so when you restart the FortiGate unit, the data is cleared. Application monitor data is stored on the hard drive and restarting the system does not affect old monitor data.

Application monitor allows you to choose to compile data for any or all of three charts: top ten applications by bandwidth use, top ten media users by bandwidth, and top ten P2P users by bandwidth. Further, there is a chart of each type for the traffic handled by each security policy with application monitor enabled. The top application usage dashboard widget shows only the bandwidth used by the top applications since the last system restart.

Enable application control

Application control examines your network traffic for traffic generated by the applications you want it to control.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an application sensor.
2. Configure the sensor to include the signatures for the application traffic you want the FortiGate unit to detect.
3. Enable any other applicable options.
4. Enable application control in a security policy and select the application sensor.

Creating an application sensor

You need to create an application sensor before you can enable application control.

To create an application sensor

1. Go to **Security Profiles > Application Control.**
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter the name of the new application sensor.
4. Optionally, you may also enter a comment.

Adding applications to an application sensor

Once you have created an application sensor, you need to need to define the applications that you want to control. You can add applications using categories and/or application overrides. Categories will allow you to choose groups of signatures based on a category type. Application overrides allow you to choose individual applications.

To add a category of signatures to the sensor.

1. Go to **Security Profiles > Application Control**.
2. In the Category section, you can select 0 or more of the following categories.
   - Botnet
   - Business
   - Cloud.IT
   - Collaboration
   - Email
   - Game
   - General.Interest
   - IM
   - Network.Service
   - P2P
   - Proxy
   - Remote.Access
   - Social.Media
   - Storage.Backup
   - Update
   - Video/Audio
   - VoIP
   - Industrial
   - Web.Others

- All Other Known Applications
- All Other Unknown Applications
  When selecting the category that you intend to work with, left click on the category name to produce a drop down menu that includes:

- Allow
- Monitor
- Block
- Reset
- Traffic Shaping
- View Signatures

3. If you wish to add individual applications, use the Application Overrides widget.
   a. Select the **Add Signatures** icon
   b. Use the Search field to narrow down the list of possible signatures.
   c. Select the Use Selected Signatures.
4. Select, if applicable from the following options:
   - Deep Inspection of Cloud Applications
   - Allow and Log DNS Traffic
   - Replacement Messages for HTTP-based Applications
5. Select Apply

Creating a New Custom Application Signature

If you have to deal with an application that is not already in the **Application List** you have the option to create a new one.

1. Go to **Security Profiles > Application Control**.
2. Select the link in the upper right corner, **[View Application Signatures]**
3. Select the **Create New** icon
4. Give the new signature a name (no spaces) in the **Name** field.
5. Enter a brief description in the **Comments** field
6. Enter the text for the signature in the signature field. Use the rules found in the Custom IPS signature chapter to determine syntax.
7. Select **OK.**

Enabling application traffic shaping

Enabling traffic shaping in an application sensor involves selecting the required shaper. You can create or edit shapers in **Policy & Objects > Objects > Traffic Shapers**.

To enable traffic shaping

1. Go to **Security Profiles > Application Control.**
2. Select application signature(s) or category(s) from the Application Control sensor.
   a. If a category is selected, left click on the category. Select Traffic Shaping. Select the desired Traffic Shaper.
3. Select **Apply**.

Any security policy with this application sensor selected will shape application traffic according to the applications specified in the list entry and the shaper configuration.

Messages in response to blocked applications

Once an Application Control sensor has been configured to block a specified application and applied to a policy it would seem inevitable that at some point an application will end up getting blocked, even if it is only to test the functionality of the control. When this happens, the sensor can be set to either display a message to offending user or to just block without any notification. The default setting is to display a message. Setting this up is done in the CLI.

```
config application list
   edit <name of the sensor>
      set app-replacemsg {enable | disable}
   end
```

Application control examples

To help give a better understanding of how to implement Application Control and to give some ideas as to why it would be used, a number of examples of scenarios are included.

Blocking all instant messaging

Instant messaging use is not permitted at the Example Corporation. Application control helps enforce this policy.

First you will create an application sensor with a single entry that includes all instant messaging applications. You will set the list action to block.

To create the application sensor

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter `no_IM` for the application sensor name.
4. Left-click on the **IM** category.
5. From the dropdown select **Block**.
6. Select **OK** to save the new sensor.

Next you will assign the sensor to a policy.

To enable application control and select the application sensor

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select the security policy that allows the network users to access the Internet and choose **Edit**.
3. Under the heading **Security Profiles** toggle the button next to **Application Control** to turn it on.
4. In the drop down menu field next to the **Application Control** select the **no_IM** application sensor.
5. Select **OK**.

No IM use will be allowed by the security policy. If other firewall policies handle traffic that users could use for IM, enable application control with the **no IM** application sensor for those as well.

Allowing only software updates

Some departments at Example Corporation do not require access to the Internet to perform their duties. Management therefore decided to block their Internet access. Software updates quickly became an issue because automatic updates will not function without Internet access and manual application of updates is time-consuming.

The solution is configuring application control to allow only automatic software updates to access the Internet.

To create an application sensor — web-based manager

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter `Updates_Only` as the application sensor name.
4. Using the left-click and drop down on the items in the **Category** list…
   a. Select **Monitor** from the dropdown menu.
   b. Select **Block** for the rest of the categories.
5. Select **OK**.

To create an application sensor — CLI

```
config application list
   edit Updates_Only
      config entries
         edit 1
            set category 17
            set action pass
         end
      set other-application-action block
      set unknown-application-action block
   end
```

You will notice that there are some differences in the naming convention between the Web Based Interface and the CLI. For instance the **Action** in the CLI is "`pass`" and the **Action** in the Web Based Manager is "**Monitor".**

Selecting the application sensor in a security policy

An application sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an application sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the application sensor in a security policy — web-based manager

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select a policy.
3. Select the **Edit** icon.
4. Under the heading **Security Profiles** toggle the button next to **Application Control** to turn it on.
5. In the drop down menu field next to the **Application Control** select the `Updates_only` list.
6. Select **OK**.

To select the application sensor in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set profile-protocol-options default
      set application-list Updates_Only
   end
```

Traffic handled by the security policy you modified will be scanned for application traffic. Software updates are permitted and all other application traffic is blocked.

Intrusion protection

The FortiGate Intrusion Protection system combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

This section describes how to configure the FortiGate Intrusion Protection settings.

If you enable virtual domains (VDOMs) on the FortiGate unit, intrusion protection is configured separately for each virtual domain.

The following topics are included:

- IPS concepts
- Enable IPS scanning
- Configure IPS options
- Enable IPS packet logging
- IPS examples

IPS concepts

The FortiGate intrusion protection system protects your network from outside attacks. Your FortiGate unit has two techniques to deal with these attacks: anomaly- and signature-based defense.

Anomaly-based defense

Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host inaccessible. The most common example is the denial of service (DoS) attack, in which an attacker directs a large number of computers to attempt normal access of the target system. If enough access attempts are made, the target is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but it is not accessible to anyone else.

The FortiGate DoS feature will block traffic above a certain threshold from the attacker and allow connections from other legitimate users. The DoS policy configuration information can be found in the Firewall Handbook.

Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access and this communication will include particular commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiGate unit to detect and stop the attack.

Signatures

IPS signatures are the basis of signature-based intrusion protection. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information so your FortiGate unit knows what to look for in network traffic.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol in which the attack will appear, the vulnerable operating system, and the vulnerable application.

To view the complete list of signatures, go to **Security Profiles > Intrusion Protection > IPS Signatures**. This will include the predefined signatures and any custom signatures that you may have created.

Protocol decoders

Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiGate unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiGate unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.

IPS engine

Once the protocol decoders separate the network traffic by protocol, the IPS engine examines the network traffic for the attack signatures.

IPS sensors

The IPS engine does not examine network traffic for all signatures, however. You must first create an IPS sensor and specify which signatures are included. Add signatures to sensors individually using signature entries, or in groups using IPS filters.

To view the IPS sensors, go to **Security Profiles > Intrusion Protection > IPS Sensor**.

IPS filters

IPS sensors contain one or more IPS filters. A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS filter.

For example, if your FortiGate unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting **OS** to **Linux**, and **Application** to **Apache,** the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS sensor, go to **Security Profiles > Intrusion Protection > IPS Sensor**, select the IPS sensor containing the filters you want to view, and choose **Edit**.

Custom/predefined signature entries

Signature entries allow you to add an individual custom or predefined IPS signature. If you need only one signature, adding a signature entry to an IPS sensor is the easiest way. Signature entries are also the only way to include custom signatures in an IPS sensor.

Another use for signature entries are to change the settings of individual signatures that are already included in a filter within the same IPS sensor. Add a signature entry with the required settings above the filter, and the signature entry will take priority.

Policies

To use an IPS sensor, you must select it in a security policy or an interface policy. An IPS sensor that it not selected in a policy will have no effect on network traffic.

IPS is most often configured as part of a security policy. Unless stated otherwise, discussion of IPS sensor use will be in regards to firewall policies in this document.

Enable IPS scanning

Enabling IPS scanning involves two separate parts of the FortiGate unit:

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day. Firewall policies can also be used to deny traffic, but those policies do not apply to IPS scanning.
- The IPS sensor contains filters, signature entries, or both. These specify which signatures are included in the IPS sensor.

When IPS is enabled, an IPS sensor is selected in a security policy, and all network traffic matching the policy will be checked for the signatures in the IPS sensor.

General configuration steps

For best results in configuring IPS scanning, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an IPS sensor.
2. Add signatures and /or filters.
   These can be:
   - Pattern based
   - Rate based
   - Customized
3. Select a security policy or create a new one.
4. In the security policy, turn on **IPS**, and choose the IPS sensor from the list.

All the network traffic controlled by this security policy will be processed according to the settings in the policy. These settings include the IPS sensor you specify in the policy.

Creating an IPS sensor

You need to create an IPS sensor before specific signatures or filters can be choosen. The signatures can be added to a new sensor before it is saved, but it is a good practice to keep in mind that the sensor and its included filters are separte things, and therefore their creation will be treated separately.

To create a new IPS sensor

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the **Create New** icon in the top of the Edit IPS Sensor window.
3. Enter the name of the new IPS sensor.
4. Optionally, you may also enter a comment. The comment will appear in the IPS sensor list and serves to remind you of the details of the sensor.
5. Select **OK**.

A newly created sensor is empty and contains no filters or signatures. You need to add one or more filters or signatures before the sensor will be of any use.

Adding an IPS filter to a sensor

While individual signatures can be added to a sensor, a filter allows you to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added.

To create a new Pattern Based Signature and Filter

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the IPS sensor to which you want to add the filter using the drop-down list in the top row of the Edit IPS Sensor window or by going to the list window.
3. In the **Pattern Based Signature and Filter** widget, select the **Create New** icon
4. For **Sensor Type** chose **Filter Based**.
5. Configure the filter that you require. Signatures matching all of the characteristics you specify in the filter will be included in the filter. Select Specify and choose the filter option that have the appropriate parameters.

Basic

Severity

Refers to the level of threat possed by the attack.

The options include:

- critical
- high
- medium
- low
- info

Target

Refers to the type of device targeted by the attack.

The options include:

- client
- server

OS

Refers to the Operating System affected by the attack.

The options include:

BSD	Linux	MacOS
Other	Solaris	Windows

Advanced

Application

Refers to the vendor or or type of application affected by the attack.

The options include:.

Adobe	Apache	Apple
CGI_app	Cisco	HP
IBM	IE	IIS
Mozilla	MS_Office	Novel
Oracle	PHP_app	Sun

This list can be expanded to include more options by selecting the [show more…] link. The additional options include:

ASP_app	CA	DB2
IM	Ipswitch	MailEnable
MediaPlayer	MS_Exchange	MSSQL
MySQL	Netscape	P2P
PostgreSQL	Real	Samba
SAP	SCADA	Sendmail
Veritas	Winamp	Other

Protocol

Refers to the protocol that is the vector for the attack.

The options include:

DNS	FTP	HTTP
ICMP	IMAP	LDAP
POP3	SCCP	SIP
SMTP	SNMP	SSH
SSL	TCP	UDP

This list can be expanded to include more options by selecting the [show more…] link. The additional options include:

BO	DCERPC	DHCP
DNP3	H323	IM
MSSQL	NBSS	NNTP
P2P	RADIUS	RDT
RPC	TRCP	RTP
RTSP	TELNET	TFN
Other		

6. Choose an action for when a signature is triggered.

Action	Description
Signature Default	All predefined signatures have an **Action** attribute that is set to Pass or Drop. This means that if a signature included in the filter has an **Action** setting of Pass, traffic matching the signature will be detected and then allowed to continue to its destination. Select **Accept signature defaults** use the default action for each included signature. **Note:** to see what the default for a signature is, go to the **IPS Signatures** page and enable the column **Action**, then find the row with the signature name in it.
Monitor All	Select **Monitor all** to pass all traffic matching the signatures included in the filter, regardless of their default **Action** setting.
Block All	Select Block all to drop traffic matching any the signatures included in the filter.
Reset	Select Reset to reset the session whenever the signature is triggered. In the CLI this action is referred to as Reject.
Quarantine	The quarantine based on the attacker's IP Address - Traffic from the Attacker's IP address is refused until the expiration time from the trigger is reached. 2. Expires (time frame that the quarantine will be in effect): • 5 Minute(s) • 30 Minutes(s) • 1 Hour(s) • 1 Day(s) • 1 Week(s) • 1 Month(s)
Packet Logging	Select to enable packet logging for the filter. When you enable packet logging on a filter, the unit saves a copy of the packets that match any signatures included in the filter. The packets can be analyzed later. For more information about packet filtering, see "Configuring packet logging options"

7. Select **OK**.

The filter is created and added to the filter list.

Adding Rate Based Signatures

These are a subset of the signatures that are found in the database that are normally set to monitor. This group of signetures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, a little like DoS attacks.

Adding a rate based signature is straight forward. Select the enable button in the Rate Based Signature table that corresponds with the desired signature.

Customized signatures

Customized signatures must be created before they can be added to the sensor. To get more details on customized signatures check the IPS Signatures chapter.

Updating predefined IPS signatures

The FortiGuard Service periodically updates the pre-defined signatures and adds new signatures to counter emerging threats as they appear.

Because the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Viewing and searching predefined IPS signatures

Go to **Security Profiles > Intrusion Protection.** Select **[View IPS Signatures]** to view the list of existing IPS signatures. You may find signatures by paging manually through the list, apply filters, or by using the search field.

Searching manually

Signatures are displayed in a paged list, with 50 signatures per page. The bottom of the screen shows the current page and the total number of pages. You can enter a page number and press enter, to skip directly to that page. Previous Page and Next Page buttons move you through the list, one page at a time. The First Page and Last Page button take you to the beginning or end of the list.

Applying filters

You can enter criteria for one of more columns, and only the signatures matching all the conditions you specify will be listed.

To apply filters

1. Go to **Security Profiles > Intrusion Protection.** Select **[View IPS Signatures] .**
2. Select column by which to filter.
3. Select the funnel/filter icon and enter the value or values to filter by.
4. Use additional columns as needed to refine search.

The available options vary by column. For example, Enable allows you to choose between two options, while OS has multiple options, and you may select multiple items together. Filtering by name allows you to enter a text string and all signature names containing the string will be displayed.

IPS processing in an HA cluster

IPS processing in an HA cluster is no different than with a single FortiGate unit, from the point of view of the network user. The difference appears when a secondary unit takes over from the primary, and what happens depends on the HA mode.

Active-passive

In an active-passive HA cluster, the primary unit processes all traffic just as it would in a stand-alone configuration. Should the primary unit fail, a secondary unit will assume the role of the primary unit and begin to process network traffic. By default, the state of active communication sessions are not shared with secondary units and will not survive the fail-over condition. Once the sessions are reestablished however, traffic processing will continue as normal.

If your network requires that active sessions are taken over by the new primary unit, select **Enable Session Pick-up** in your HA configuration. Because session information must be sent to all subordinate units on a regular basis, session pick-up is a resource-intensive feature and is not enabled by default.

Active-active

The fail-over process in an active-active cluster is similar to an active-passive cluster. When the primary unit fails, a secondary unit takes over and traffic processing continues. The load-balancing schedule used to distribute sessions to the cluster members is used by the new primary unit to redistribute sessions among the remaining subordinate units. If session pick-up is not enabled, the sessions active on the failed primary are lost, and the sessions redistributed among the secondary units may also be lost. If session pick-up is enabled, all sessions are handled according to their last-known state.

Configure IPS options

There are a number of CLI commands that influence how IPS functions.

Hardware Acceleration

In order to provide control over the hardware's processing of IPS there are commands to configure and control the hardware accelleration of IPS. There are two settings that can be chosen, one for the network processor and one for the content processor.

Network processor acceleration can be disabled or set to enable basic acceleration.

Content processor acceleration can be disabled or set to either basic or advanced acceleration.

These Settings are only found in the CLI:

```
config ips global
   set np-accel-mode {none | basic}
   set cp-accel-mode {none | basic | advanced}
end
```

Extended IPS Database.

Some models have access to an extended IPS Database. The extended database may affect the performance of the FortiGate unit so depending on the model of the FortiGate unit the extended database package may not be enabled by default. For example, the D-series Desktop model have this option disabled by default.

This feature can only be enbled through the CLI.

```
config ips global
   set database extended
end
```

Configuring the IPS engine algorithm

The IPS engine is able to search for signature matches in two ways. One method is faster but uses more memory, the other uses less memory but is slower. Use the `algorithm` CLI command to select one method:

```
config ips global
   set algorithm {super | high | low | engine-pick}
end
```

Specify `high` to use the faster more memory intensive method or `low` for the slower memory efficient method. The setting `super` improves the performance for FortiGate units with more than 4GB of memory. The default setting is `engine-pick`, which allows the IPS engine to choose the best method on the fly.

Configuring the IPS engine-count

FortiGate units with multiple processors can run more than one IPS engine concurrently. The `engine-count` CLI command allows you to specify how many IPS engines are used at the same time:

```
config ips global
   set engine-count <int>
end
```

The recommended and default setting is `0`, which allows the FortiGate unit to determine the optimum number of IPS engines.

Configuring fail-open

If the IPS engine fails for any reason, it will fail open by default. This applies for inspection of all the protocols inspected by FortiOS IPS protocol decoders, including but not limited to HTTP, HTTPS, FTP, SMTP, POP3, IMAP, etc. This means that traffic continues to flow without IPS scanning. If IPS protection is more important to your network than the uninterrupted flow if network traffic, you can disable this behavior using the `fail-open` CLI command:

```
config ips global
   set fail-open {enable | disable}
end
```

The default setting is disable.

Configuring the session count accuracy

The IPS engine can keep track of the number of open session in two ways. An accurate count uses more resources than a less accurate heuristic count.

```
config ips global
```

```
   set session-limit-mode {accurate | heuristic}
end
```

The default is heuristic.

Configuring IPS intelligence

If `intelligent-mode` is enabled (the default), in most cases the IPS engine will scan the first 200 kilobytes of a session (this value is hard coded).

In some cases, however, the IPS engine will still scan all traffic in a session. If `intelligent-mode` is disabled, the IPS engine scans all traffic.

```
config ips global
   set intelligent-mode [enable|disable]
end
```

Configuring the IPS buffer size

Set the size of the IPS buffer.

```
config ips global
   set socket-size <int>
end
```

The acceptable range is from 1 to 64 megabytes. The default size varies by model. In short, `socket-size` determines how much data the kernel passes to the IPS engine each time the engine samples packets.

Configuring protocol decoders

The FortiGate Intrusion Protection system uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

To change the ports a decoder examines, you must use the CLI. In this example, the ports examined by the DNS decoder are changed from the default 53 to 100, 200, and 300.

```
config ips decoder dns_decoder
   set port_list "100,200,300"
end
```

You cannot assign specific ports to decoders that are set to **auto** by default. These decoders can detect their traffic on any port. Specifying individual ports is not necessary.

Configuring security processing modules

FortiGate Security Processing Modules, such as the CE4, XE2, and FE8, can increase overall system performance by accelerating some security and networking processing on the interfaces they provide. They also allow the FortiGate unit to offload the processing to the security module, thereby freeing up its own processor for other tasks. The security module performs its own IPS and firewall processing, but you can configure it to favor IPS in hostile high-traffic environments.

If you have a security processing module, use the following CLI commands to configure it to devote more resources to IPS than firewall. This example shows the CLI commands required to configure a security module in slot 1 for increased IPS performance.

```
config system amc-slot
```

```
edit sw1
   set optimization-mode fw-ips
   set ips-weight balanced
   set ips-p2p disable
   set ips-fail-open enable
   set fp-disable none
   set ipsec-inb-optimization enable
   set syn-proxy-client-timer 3
   set syn-proxy-server-timer 3
end
```

In addition to offloading IPS processing, security processing modules provide a hardware accelerated SYN proxy to defend against SYN flood denial of service attacks. When using a security module, configure your DoS anomaly check for `tcp_syn_flood` with the **Proxy** action. The **Proxy** action activates the hardware accelerated SYN proxy.

IPS signature rate count threshold

The IPS signature threshold can allow configuring a signature so that it will not be triggered until a rate count threshold is met. This provides a more controlled recording of attack activity. For example, if multiple login attempts produce a failed result over a short period of time then an alert would be sent and perhaps traffic blocked. This would be a more rational response than sending an alert every time a login failed.

The syntax for this configuration is as follows:

```
config ips sensor
   edit default
      config entries
         edit <Filter ID number>
            set rule <*id>
            set rate-count <integer between 1 - 65535>
            set rate-duration <integer between 1 - 65535>
```

The value of the rate-duration is an integer for the time in seconds.

```
set rate-mode <continuous | periodical>
```

The rate-mode refers to how the count threshold is met.

If the setting is "`continuous`", and the action is set to block, as soon as the `rate-count` is reached the action is engaged. For example, if the count is 10, as soon as the signature is triggered 10 times the traffic would be blocked.

If the setting is "periodical", the FortiGate allows up to the value of the rate-count incidents where the signature is triggered during the rate-duration. For example, if the rate count is 100 and the duration is 60, the signature would need to be triggered 100 times in 60 seconds for the action to be engaged.

```
set rate-track <dest-ip | dhcp-client-mac | dns-domain | none | src-ip>
```

This setting allows the tracking of one of the protocol fields within the packet.

Enable IPS packet logging

Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging in the filters. Use caution in enabling packet logging in a filter. Filters configured with few restrictions can contain thousands of signatures, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.

To enable packet logging for a filter

1. Create a filter in an IPS sensor.
2. Before saving the filter, check the box next to **Packet Logging** just under the filter action options.
3. Select the IPS sensor in the security policy that allows the network traffic the FortiGate unit will examine for the signature.

For information on viewing and saving logged packets, see "Configuring packet logging options".

IPS examples

Configuring basic IPS protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable IPS protection on a FortiGate unit located in a satellite office. The satellite office contains only Windows clients.

Creating an IPS sensor

Most IPS settings are configured in an IPS sensor. IPS sensors are selected in firewall policies. This way, you can create multiple IPS sensors, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one IPS sensor.

To create an IPS sensor— web-based manager

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the **Create New** icon in the top of the Edit IPS Sensor window.
3. In the **Name** field, enter `basic_ips`.
4. In the **Comments** field, enter `IPS protection for Windows clients.`
5. Select **OK**.
6. Select the **Create New** drop-down to add a new component to the sensor and for the **Sensor Type** choose **Filter** Based.
7. In the Filter Options choose the following:
   a. For **Severity**: select all of the options
   b. For **Target**: select **Client** only.
   c. For **OS**: select **Windows** only.
8. For the **Action** leave as the default.
9. Select **OK** to save the filter.

10. Select **OK** to save the IPS sensor.

To create an IPS sensor — CLI

```
config ips sensor
   edit basic_ips
      set comment "IPS protection for Windows clients"
         config entries
            edit 1
               set location client
               set os windows
         end
   end
```

Selecting the IPS sensor in a security policy

An IPS sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an IPS sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the IPS sensor in a security policy — web-based manager

1. Go to **Policy > Policy > Policy**.
2. Select a policy.
3. Select the **Edit** icon.
4. Enable the **IPS** option.
5. Select the `basic_ips` profile from the list.
6. Select **OK** to save the security policy.

To select the IPS sensor in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set ips-sensor basic_ips
   end
```

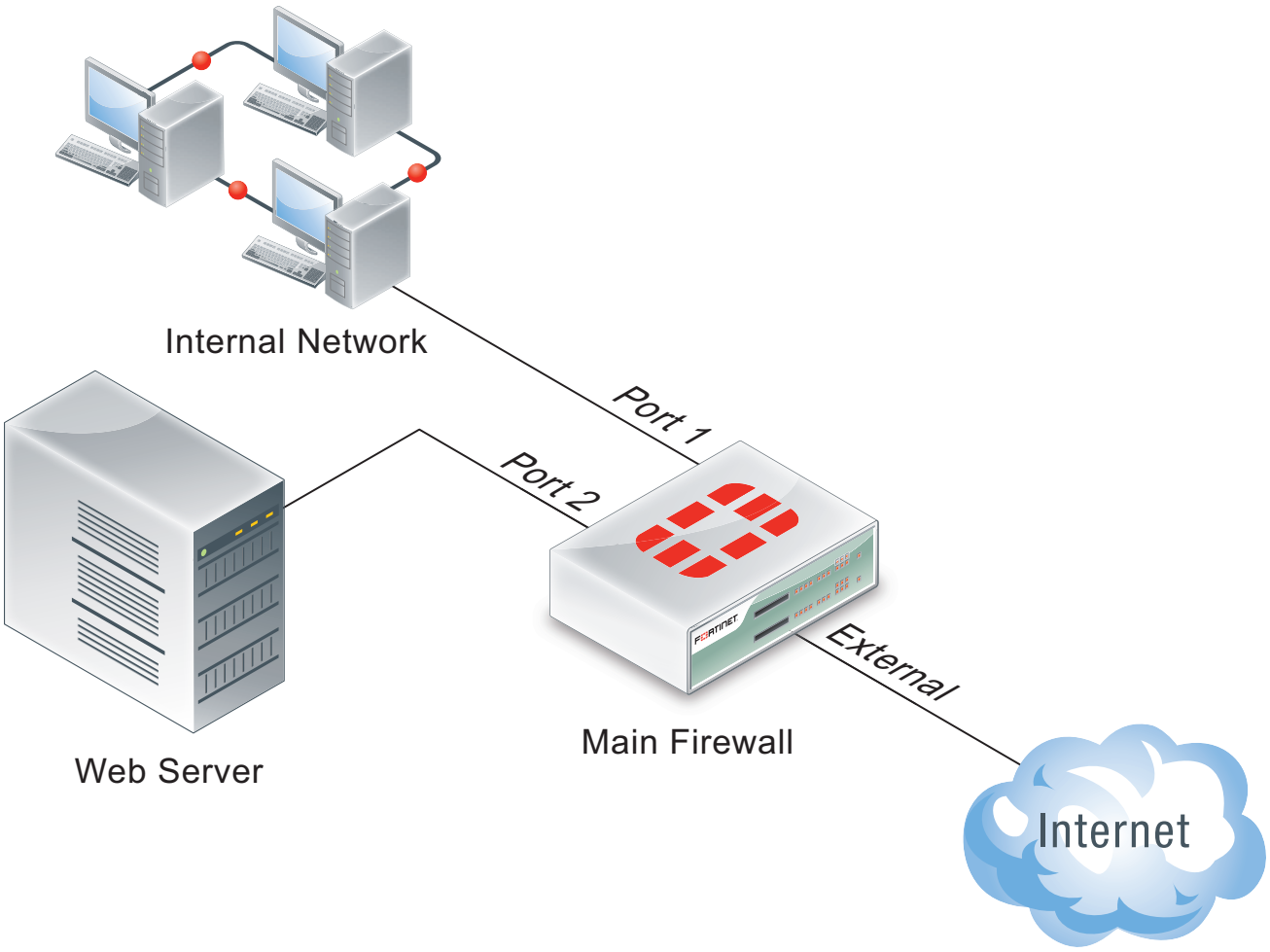
All traffic handled by the security policy you modified will be scanned for attacks against Windows clients. A small office may have only one security policy configured. If you have multiple policies, consider enabling IPS scanning for all of them.

Using IPS to protect your web server

Many companies have web servers and they must be protected from attack. Since web servers must be accessible, protection is not as simple as blocking access. IPS is one tool your FortiGate unit has to allow you to protect your network.

In this example, we will configure IPS to protect a web server. As shown below, a FortiGate unit protects a web server and an internal network. The internal network will have its own policies and configuration but we will concentrate on the web server in this example.

A simple network configuration



The FortiGate unit is configured with:

- a virtual IP to give the web server a unique address accessible from the Internet.
- a security policy to allow access to the web server from the Internet using the virtual IP.

To protect the web server using intrusion protection, you need to create an IPS sensor, populate it with filters, then enable IPS scanning in the security policy.

To create an IPS sensor

1. Go to **Security Profiles > Intrusion Protection.**
2. Select **Create New**.
3. Enter `web_server` as the name of the new IPS sensor.
4. Select **OK**.

The new IPS sensor is created but it has no filters, and therefore no signatures are included.

The web server operating system is Linux, so you need to create a filter for all Linux server signatures.

To create the Linux server filter

1. Go to **Security Profiles > Intrusion Protection.**
2. Select the `web_server` IPS sensor and select the **Edit** icon.
3. In the **Pattern Based Signatures and Filters** section, select **Create New**.
4. For **Sensor Type**, select **Filter Based.**
5. For Filter **Options**.
6. In the Filter Options choose the following:
   a. For **Severity**: select all of the options
   b. For **Target**: select **server** only.
   c. For **OS**: select **Linux** only.
7. Select **OK**.

The filter is saved and the IPS sensor page reappears. In the filter list, find the **Linux Server** filter and look at the value in the **Count** column. This shows how many signatures match the current filter settings. You can select the **View Rules** icon to see a listing of the included signatures.

To edit the security policy

1. Go to **Policy > Policy > IPv4** select security policy that allows access to the web server, and select the **Edit** icon.
2. Enable IPS option and choose the `web_server` IPS sensor from the list.
3. Select **OK**.

Since IPS is enabled and the `web_server` IPS sensor is specified in the security policy controlling the web server traffic, the IPS sensor examines the web server traffic for matches to the signatures it contains.

Create and test a packet logging IPS sensor

In this example, you create a new IPS sensor and include a filter that detects the EICAR test file and saves a packet log when it is found. This is an ideal first experience with packet logging because the EICAR test file can cause no harm, and it is freely available for testing purposes.

Create an IPS senor

1. Go to **Security Profiles > Intrusion Protection**.
2. Select **Create New**.
3. Name the new IPS sensor `EICAR_test`.
4. Select **OK**.

Create an entry

1. Select the **Create New**.
2. For **Sensor Type** choose **Specify Signatures**.
3. Rather than search through the signature list, use the name filter by selecting the search icon over the header of the **Signature** column.
4. Enter `EICAR` in the Search field.
5. Highlight the `Eicar.Virus.Test.File` signature by clicking on it.
6. Select **Block All** as the **Action**.

7. Enable **Packet Logging.**
8. Select OK to save the IPS sensor.

You are returned to the IPS sensor list. The `EICAR test` sensor appears in the list.

Add the IPS sensor to the security policy allowing Internet access

1. Go to **Policy > Policy > IPv4**.
2. Select the security policy that allows you to access the Internet.
3. Select the **Edit** icon.
4. Turn ON **Log Allowed Traffic**.
   a. Select All Sessions
5. Enable the **IPS** option.
6. Choose `EICAR test` from the available IPS sensors.
7. Select **OK**.

With the IPS sensor configured and selected in the security policy, the FortiGate unit blocks any attempt to download the EICAR test file.

Test the IPS sensor

1. Using your web browser, go to http://www.eicar.org/anti_virus_test_file.htm.
2. Scroll to the bottom of the page and select **eicar.com** from the row labeled as using the standard HTTP protocol.
3. The browser attempts to download the requested file and,
   - If the file is successfully downloaded, the custom signature configuration failed at some point. Check the custom signature, the IPS sensor, and the firewall profile.
   - If the download is blocked with a high security alert message explaining that you're not permitted to download the file, the EICAR test file was blocked by the FortiGate unit antivirus scanner before the IPS sensor could examine it. Disable antivirus scanning and try to download the EICAR test file again.
   - If no file is downloaded and the browser eventually times out, the custom signature successfully detected the EICAR test file and blocked the download.

Viewing the packet log

1. Go to **Log&Report > Security Log > AntiVirus**.
2. Locate the log entry that recorded the blocking of the EICAR test file block. The Message field data will be `tools: EICAR.AV.Test.File.Download`.
3. Select the **View Packet Log** icon in the **Packet Log** column.
4. The packet log viewer is displayed.

Configuring a Fortinet Security Processing module

The Example Corporation has a web site that is the target of SYN floods. While they investigate the source of the attacks, it's very important that the web site remain accessible. To enhance the ability of the company's FortiGate-620B to deal with SYN floods, the administrator will install an ASM-CE4 Fortinet Security Processing module and have all external access to the web server come though it.

The security processing modules not only accelerate and offload network traffic from the FortiGate unit's processor, but they also accelerate and offload security and content scanning. The ability of the security module to accelerate IPS scanning and DoS protection greatly enhances the defense capabilities of the FortiGate-620B.

Assumptions

As shown in other examples and network diagrams throughout this document, the Example Corporation has a pair of FortiGate-620B units in an HA cluster. To simplify this example, the cluster is replaced with a single FortiGate-620B.

An ASM-CE4 is installed in the FortiGate-620B.

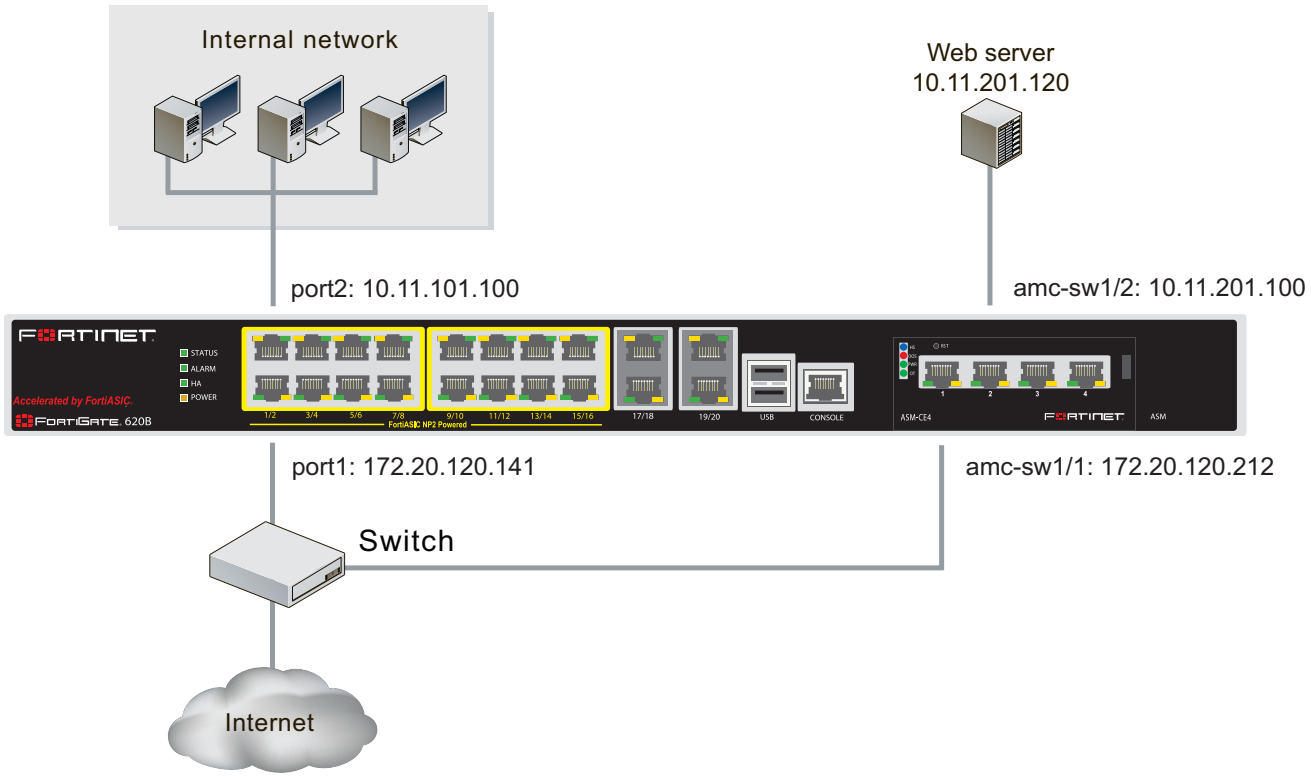
The network is configured as shown below.

Network configuration

The Example Corporation network needs minimal changes to incorporate the ASM-CE4. Interface amc-sw1/1 of the ASM-CE4 is connected to the Internet and interface amc-sw1/1 is connected to the web server.

Since the main office network is connected to port2 and the Internet is connected to port1, a switch is installed to allow both port1 and amc-sw1/1 to be connected to the Internet.

The FortiGate-620B network configuration



The switch used to connect port1 and amc-sw1/1 to the Internet must be able to handle any SYN flood, all of the legitimate traffic to the web site, and all of the traffic to and from the Example Corporation internal network. If the switch can not handle the bandwidth, or if the connection to the service provider can not provide the required bandwidth, traffic will be lost.

Security module configuration

The Fortinet security modules come configured to give equal priority to content inspection and firewall processing. The Example Corporation is using a ASM-CE4 module to defend its web server against SYN flood attacks so firewall processing is a secondary consideration.

Use these CLI commands to configure the security module in ASM slot 1 to devote more resources to content processing, including DoS and IPS, than to firewall processing.

```
config system amc-slot
   edit sw1
      set optimization-mode fw-ips
      set ips-weight balanced
      set ips-p2p disable
      set ips-fail-open enable
      set fp-disable none
      set ipsec-inb-optimization enable
      set syn-proxy-client-timer 3
      set syn-proxy-server-timer 3
   end
```

These settings do not disable firewall processing. Rather, when the security module nears its processing capacity, it will chose to service content inspection over firewall processing.

IPS Sensor

You can group signatures into IPS sensors for easy selection when applying to firewall policies. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic. For example, you can specify all of the web-server related signatures in an IPS sensor, and that sensor can then be applied to a firewall policy that controls all of the traffic to and from a web server protected by the unit.

The FortiGuard Service periodically updates the pre-defined signatures, with signatures added to counter new threats. Since the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Each IPS sensor consists of two parts: filters and overrides. Overrides are always checked before filters.

Each filter consists of a number of signatures attributes. All of the signatures with those attributes, and only those attributes, are checked against traffic when the filter is run. If multiple filters are defined in an IPS Sensor, they are checked against the traffic one at a time, from top to bottom. If a match is found, the unit takes the appropriate action and stops further checking.

A signature override can modify the behavior of a signature specified in a filter. A signature override can also add a signature not specified in the sensor's filters. Custom signatures are included in an IPS sensor using overrides.

The signatures in the overrides are first compared to network traffic. If the IPS sensor does not find any matches, it then compares the signatures in each filter to network traffic, one filter at a time, from top to bottom. If no signature matches are found, the IPS sensor allows the network traffic.

The signatures included in the filter are only those matching every attribute specified. When created, a new filter has every attribute set to **all** which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

Custom Application & IPS Signatures

Creating a custom IPS signature

The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can add or edit custom signatures using the web-based manager or the CLI.

To create a custom signature

1. Go to **Security Profiles > Intrusion Protection**.
2. Select **[View IPS Signatures]**
3. Select **Creat New** to add a new custom signature.
4. Enter a **Name** for the custom signature.
5. Enter the **Signature**. For information about completing this field, see “Custom signature syntax and keywords”.
6. Select **OK**.

Custom signature syntax and keywords

All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.

Custom signature syntax

A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)

You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to **Security Profiles > Intrusion Protection > IPS Signatues,** select **Create New** and enter the data directly into the **Signature** field, following the guidance in the next topics.

The table below shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords”.

Valid syntax for custom signature fields

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Custom signature keywords

Information keywords

attack_id

Syntax: `--attack_id <id_int>;`

Description:

Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiGate automatically assigns an attack ID to the signature. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs.

An attack ID you assign must be between 1000 and 9999.

Example: --attack_id 1234;

name

Syntax: `--name <name_str>;`

Description:

Enter the name of the rule. A rule name must be unique. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same rule name for signatures in different VDOMs. The name you assign must be a string greater than 0 and less than 64 characters in length.

Example: `--name "Buffer_Overflow";`

Session keywords

flow

Syntax: `--flow {from_client[,reversed] | from_server[,reversed] | bi_direction };`

Description:

Specify the traffic direction and state to be inspected. They can be used for all IP traffic.

Example: `--src_port 41523; --flow bi_direction;`

The signature checks traffic to and from port 41523.

If you enable “quarantine attacker”, the optional reversed keyword allows you to change the side of the connection to be quarantined when the signature is detected.

For example, a custom signature written to detect a brute-force log in attack is triggered when “Login Failed” is detected from_server more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker.

Previous FortiOS versions used to_client and to_server values. These are now deprecated, but still function for backwards compatibility.

service

Syntax: `--service {HTTP | TELNET | FTP | DNS | SMTP | POP3 | IMAP | SNMP | RADIUS | LDAP | MSSQL | RPC | SIP | H323 | NBSS | DCERPC | SSH | SSL};`

Description:

Specify the protocol type to be inspected. This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content.

Content keywords

byte_jump

Syntax: `--byte_jump <bytes_to_convert>, <offset>[, multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct] [, align];`

Description:

Use the `byte_jump` option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data.

The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to examine from the packet.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.
- `align`: Round up the number of converted bytes to the next 32-bit boundary.

byte_test

Syntax: `--byte_test <bytes_to_convert>, <operator>, <value>, <offset> [multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct];`

Description:

Use the `byte_test` keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to compare.
- `<operator>`: The operation to perform when comparing the value (<,>,=,!,&).
- `<value>`: The value to compare the converted value against.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.

depth

Syntax: `--depth <depth_int>;`

Description:

Use the depth keyword to search for the contents within the specified number of bytes after the starting point defined by the offset keyword. If no offset is specified, the offset is assumed to be equal to 0.

If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched.

The depth must be between 0 and 65535.

distance

Syntax: `--distance <dist_int>;`

Description:

Use the distance keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the within keyword is not specified, continue looking for a match until the end of the payload.

The distance must be between 0 and 65535.

content

Syntax: `--content [!]"<content_str>";`

Description:

Deprecated, see pattern and context keywords. Use the content keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.

To have the FortiGate search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.

Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character.

The double quote ("), pipe sign(|) and colon(:) characters must be escaped using a back slash if specified in a content string.

If the value of the content keyword is greater than the length of the value of the depth keyword, this signature will never be matched.

context

Syntax: `--context {uri | header | body | host};`

Description:

Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiGate unit searches for the pattern anywhere in the packet buffer. The available context variables are:

- `uri`: Search for the pattern in the HTTP URI line.
- `header`: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages.
- `body`: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body.
- `host`: Search for the pattern in HTTP HOST line.

no_case

Syntax: `--no_case;`

Description:

Use the no-case keyword to force the FortiGate unit to perform a case-insensitive pattern match.

offset

Syntax: `--offset <offset_int>;`

Description:

Use the offset keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the offset keyword with the depth keyword to stop looking for a match after a specified number of bytes. If no depth is specified, the FortiGate unit continues looking for a match until the end of the payload.

The offset must be between 0 and 65535.

pattern

Syntax: `--pattern [!]"<pattern_str>";`

Description:

The FortiGate unit will search for the specified pattern. A pattern keyword normally is followed by a context keyword to define where to look for the pattern in the packet. If a context keyword is not present, the FortiGate unit looks for the pattern anywhere in the packet buffer. To have the FortiGate search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.

Example: `--pattern "/level/" --pattern "|E8 D9FF FFFF|/bin/sh" --pattern !"|20|RTSP/"`

pcre

Syntax: `--pcre [!]"/<regex>/[ismxAEGRUB]";`

Description:

Similarly to the pattern keyword, use the pcre keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A pcre keyword can be followed by a context keyword to define where to look for the pattern in the packet. If no context keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer.

For more information about PCRE syntax, go to http://www.pcre.org.

The switches include:

- `i`: Case insensitive.
- `s`: Include newlines in the dot metacharacter.
- `m`: By default, the string is treated as one big line of characters. ^ and $ match at the beginning and ending of the string. When m is set, ^ and $ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.
- `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.
- `A`: The pattern must match only at the start of the buffer (same as ^).
- `E`: Set $ to match only at the end of the subject string. Without E, $ also matches immediately before the final character if it is a newline (but not before any other newlines).

- G: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by ?.
- R: Match relative to the end of the last pattern match. (Similar to distance:0;).
- U: Deprecated, see the context keyword. Match the decoded URI buffers.

uri

Syntax: `--uri [!]"<uri_str>";`

Description:

Deprecated, see pattern and context keywords. Use the uri keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("). To have the FortiGate unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign (|) and colon (:) characters must be escaped using a back slash (\) if specified in a URI string.

within

Syntax: `--within <within_int>;`

Description:

Use this together with the distance keyword to search for the contents within the specified number of bytes of the payload.

The within value must be between 0 and 65535.

IP header keywords

dst_addr

Syntax: `--dst_addr [!]<ipv4>;`

Description:

Use the dst_addr keyword to search for the destination IP address. To have the FortiGate search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `dst_addr [172.20.0.0/16, 10.1.0.0/16,192.168.0.0/16]`

ip_id

Syntax: `--ip_id <field_int>;`

Description:

Check the IP ID field for the specified value.

ip_option

Syntax: `--ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any};`

Description:

Use the ip_option keyword to check various IP option settings.

The available options include:

- `rr`: Check if IP RR (record route) option is present.
- `eol`: Check if IP EOL (end of list) option is present.
- `nop`: Check if IP NOP (no op) option is present.
- `ts`: Check if IP TS (time stamp) option is present.
- `sec`: Check if IP SEC (IP security) option is present.
- `lsrr`: Check if IP LSRR (loose source routing) option is present.
- `ssrr`: Check if IP SSRR (strict source routing) option is present.
- `satid`: Check if IP SATID (stream identifier) option is present.
- `any`: Check if IP any option is present.

ip_tos

Syntax: `--ip_tos <field_int>;`

Description:

Check the IP TOS field for the specified value.

ip_ttl

Syntax: `--ip_ttl [< | >] <ttl_int>;`

Description:

Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol.

protocol

Syntax: `--protocol {<protocol_int> | tcp | udp | icmp};`

Description:

Check the IP protocol header.

Example: `--protocol tcp;`

src_addr

Syntax: `--src_addr [!]<ipv4>;`

Description:

Use the src_addr keyword to search for the source IP address. To have the FortiGate unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `src_addr 192.168.13.0/24`

TCP header keywords

ack

Syntax: `--ack <ack_int>;`

Description:

Check for the specified TCP acknowledge number.

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the `dst_port` keyword to specify the destination port number.

You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

seq

Syntax: `--seq [operator,]<number>[,relative];`

Description:

Check for the specified TCP sequence number.

- `operator` includes =,<,>,!.
- `relative` indicates it's relative to the initial sequence number of the TCP session.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the src_port keyword to specify the source port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

tcp_flags

Syntax: `--tcp_flags <SAFRUP120>[!|*|+] [,<SAFRUP120>];`

Description:

Specify the TCP flags to match in a packet.

- `S`: Match the SYN flag.
- `A`: Match the ACK flag.
- `F`: Match the FIN flag.
- `R`: Match the RST flag.
- `U`: Match the URG flag.
- `P`: Match the PSH flag.
- `1`: Match Reserved bit 1.
- `2`: Match Reserved bit 2.
- `0`: Match No TCP flags set.
- `!`: Match if the specified bits are not set.
- `*`: Match if any of the specified bits are set.
- `+`: Match on the specified bits, plus any others.

The first part if the value (`<SAFRUP120>`) defines the bits that must be present for a successful match.

Example:

`--tcp_flags AP` only matches the case where both `A` and `P` bits are set.

The second part (`[,<SAFRUP120>]`) is optional, and defines the additional bits that can be present for a match.

For example `tcp_flags S,12` matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2. The modifiers !, * and + cannot be used in the second part.

window_size

Syntax: `--window_size [!]<window_int>;`

Description:

Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by `0x`. To have the FortiGate search for the absence of the specified window size, add an exclamation mark (`!`) before the window size.

UDP header keywords

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

ICMP keywords

icmp_code

Syntax: `--icmp_code <code_int>;`

Description:

Specify the ICMP code to match.

icmp_id

Syntax: `--icmp_id <id_int>;`

Description:

Check for the specified ICMP ID value.

icmp_seq

Syntax: `--icmp_seq <seq_int>;`

Description:

Check for the specified ICMP sequence value.

icmp_type

Syntax: `--icmp_type <type_int>;`

Description:

Specify the ICMP type to match.

Other keywords

data_size

Syntax: `--data_size {<size_int> | <<size_int> | ><size_int>;`

Description:

Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.

- `<size_int>` is a particular packet size.
- `<<size_int>` is a packet smaller than the specified size.
- `><size_int>` is a packet larger than the specified size.

Examples:

- `--data_size 300;`
- `--data_size <300;`
- `--data_size >300;`

data_at

Syntax: `--data_at <offset_int>[, relative];`

Description:

Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.

rate

Syntax: `--rate <matches_int>,<time_int>;`

Description:

Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.

- `<matches_int>` is the number of times a signature must be detected.
- `<time_int>` is the length of time in which the signature must be detected, in seconds.

For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If `--rate 100,10;` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. Use this command with `--track` to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.

rpc_num

Syntax: `--rpc_num <app_int>[, <ver_int> | *][, <proc_int> | *>];`

Description:

Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wild card can be used for version and procedure numbers.

same_ip

Syntax: `--same_ip;`

Description:

Check that the source and the destination have the same IP addresses.

track

Syntax: `--track {SRC_IP |DST_IP |DHCP_CLIENT |DNS_DOMAIN}[,block_int];`

Description:

When used with `--rate`, this keyword narrows the custom signature rate totals to individual addresses.

- `SRC_IP`: tracks the packet's source IP.
- `DST_IP`: tracks the packet's destination IP.
- `DHCP_CLIENT`: tracks the DHCP client's MAC address.
- `DNS_DOMAIN`: counts the number of any specific domain name.
- `block_int` has the FortiGate unit block connections for the specified number of seconds, from the client or to the server, depending on which is specified.

  For example, if `--rate 100,10` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiGate unit maintains a single total, regardless of source and destination address.

  If the same custom signature also includes `--track` client; matches are totaled separately for each source address. A log entry is added when the signature is detected 100 times in 10 seconds within traffic from the same source address.

  The `--track` keyword can also be used without `--rate`. If an integer is specified, the client or server will be blocked for the specified number of seconds every time the signature is detected.

Creating a custom signature to block access to example.com

In this first example, you will create a custom signature to block access to the example.com URL.

This example describes the use of the custom signature syntax to block access to a URL. To create the custom signature entry in the FortiGate unit web-based manager, see “Creating a custom IPS signature”.

1. Enter the custom signature basic format.

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords. Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "Block.example.com"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3. Add a signature pattern

   Use the `--pattern` keyword to specify what the FortiGate unit will search for:

```
F-SBID( --name "Block.example.com"; --pattern "example.com"; )
```

The signature will now detect the example.com URL appearing in network traffic. The custom signature should only detect the URL in HTTP traffic, however. Any other traffic with the URL should be allowed to pass. For example, an email message to or from example.com should not be stopped.

4. Specify the service

   Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; )
   ```

   The FortiGate unit will limit its search for the pattern to the HTTP protocol. Even though the HTTP protocol uses only TCP traffic, the FortiGate will search for HTTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --
       protocol tcp; )
   ```

   The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network traffic.

6. Ignore case sensitivity

   By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

   Use the `--no_case` keyword to make the pattern matching case insensitive.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_
       case; )
   ```

   Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7. Limit pattern scans to only traffic sent from the client

   The `--flow` command can be used to further limit the network traffic being scanned to only that send by the client or by the server.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_
       case; --flow from_client; )
   ```

   Web servers do not contact clients until clients first open a communication session. Therefore, using the `--flow from_client` command will force the FortiGate to ignore all traffic from the server. Since the majority of HTTP traffic flows from the server to the client, this will save considerable system resources and still maintain protection.

8. Specify the context

   When the client browser tries to contact example.com, a DNS is first consulted to get the example.com server IP address. The IP address is then specified in the URL field of the HTTP communication. The domain name will still appear in the host field, so this custom signature will not function without the `--context host` keyword/value pair.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_
       case; --flow from_client; --context host; )
   ```

Creating a custom signature to block the SMTP “vrfy” command

The SMTP “vrfy” command can be used to verify the existence of a single email address or to list all of the valid email accounts on an email server. A spammer could potentially use this command to obtain a list of all valid email users and direct spam to their inboxes.

In this example, you will create a custom signature to block the use of the vrfy command. Since the custom signature blocks the vrfy command from coming through the FortiGate unit, the administrator can still use the command on the internal network.

This example describes the use of the custom signature syntax to block the vrfy command. To create the custom signature entry in the FortiGate unit web-based manager, see “Creating a custom IPS signature”.

1. Enter the custom signature basic format

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before you add any other keywords.

   Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3. Add a signature pattern

   Use the `--pattern` keyword to specify what the FortiGate unit will search for:

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; )
   ```

   The signature will now detect the vrfy command appearing in network traffic. The custom signature should only detect the command in SMTP traffic, however. Any other traffic with the pattern should be allowed to pass. For example, an email message discussing the vrfy command should not be stopped.

4. Specify the service.

   Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; )
   ```

   The FortiGate unit will limit its search for the pattern to the SMTP protocol.

   Even though the SMTP protocol uses only TCP traffic, the FortiGate will search for SMTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --
    protocol tcp; )
```

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore the pattern in UDP and ICMP network traffic.

6. Ignore case sensitivity.

   By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

   Use the `--no_case` keyword to make the pattern matching case insensitive.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --no_case; )
   ```

   Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7. Specify the context.

   The `SMTP vrfy` command will appear in the SMTP header. The `--context host` keyword/value pair allows you to limit the pattern search to only the header.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --no_case; -
       -context header; )
   ```

Creating a custom signature to block files according to the file's hash value

In this example, you will create a custom signature that allows you to specify a hash value (or checksum) of a file that you want to block. To block multiple files you can create a custom signature for each file with that file's hash value in it and then add all of the custom signatures to an IPS sensor and set the action to block for each one. When IPS encounters a file with a matching hash value the file is blocked.

This example uses a CRC32 checksum of the file as the hash value of the file to be blocked. You can use any utility that supports CRC32 checksums to generate the hash value.

1. Enter the custom signature basic format.

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords. Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "File.Hash.Example"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic.

3. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

   ```
   F-SBID( --name "File.Hash.Example"; --protocol tcp; )
   ```

   The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network traffic.

4. Add the CRC32 hash value.

   Use the `--crc32` keyword. This indicates that the value that follows is a hexadecimal number that represents the CRC32 checksum of the file. The `--crc32` keyword also requires that you include the file length. The syntax is `--crc32 <checksum>,<file-length>;`. The following example shows the syntax for a file with checksum 51480492 and file length 822.

   ```
   F-SBID( --name "File.Hash.Example"; --protocol tcp; --crc32 51480492,822; )
   ```

Email filter

This section describes how to configure FortiGate email filtering for IMAP, POP3, and SMTP email. Email filtering includes both spam filtering and filtering for any words or files you want to disallow in email messages. If your FortiGate unit supports SSL content scanning and inspection, you can also configure spam filtering for IMAPS, POP3S, and SMTPS email traffic.

The following topics are included in this section:

- Email filter concepts
- Enable email filtering
- Configure email traffic types to inspect
- Configure the spam action
- Configure the tag location
- Configure the tag format
- Configuring an Email Filters
- Configure local email filters
- Email filter examples

Email filter concepts

You can configure the FortiGate unit to manage unsolicited commercial email by detecting and identifying spam messages from known or suspected spam servers.

The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools, to detect and block a wide range of spam messages. Using FortiGuard Antispam email filter profile settings, you can enable IP address checking, URL checking, email checksum checking, and spam submission. Updates to the IP reputation and spam signature databases are provided continuously via the global FortiGuard Distribution Network.

From the FortiGuard Antispam Service page in the FortiGuard Center, you can find out whether an IP address is blacklisted in the FortiGuard antispam IP reputation database, or whether a URL or email address is in the signature database.

Email filter techniques

The FortiGate unit has a number of techniques available to help detect spam. Some use the FortiGuard Antispam Service and require a subscription. The remainder use your DNS servers or use lists that you must maintain.

Black white list

These are the types of black white lists available. They include:

- **IP/Netmask**
  The FortiGate unit compares the IP address of the client delivering the email to the addresses in the IP address black/white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry against all delivered email.
  The default setting of the `smtp-spamhdrip` CLI command is `disable`. If enabled, the FortiGate unit will check

all the IP addresses in the header of SMTP email against the specified IP address black/white list.

- **Email Wildcard**
  The FortiGate unit compares the sender email address, as shown in the message envelope MAIL FROM, to the pattern in the patterned field. The wildcard symbol is used in the patterned to replace the characters in the address that may vary from the pattern. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry.
- **Email Regular Expression**
  The FortiGate unit compares the sender email address, as shown in the message envelope MAIL FROM, to the pattern in the patterned field. The regular expression that can be used is much more sophisticated than a simple wildcard variable. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry.

Pattern

The pattern field is for entering the identifying information that will enable the filter to correctly identify the email messages.

- If the type is IP/Netmask the filter will be an IP address with a subnet mask.
- If the type is Email Wildcard the filter will be an email address with a wildcard symbol in place of the variable characters. For example *.example.com or fred@*.com.
- If the type is Email Regular Expression, regular expression can be used to create a more granular filter for email addresses. For example, ^[_a-z0-9-]+(\.[_a-z0-9-]+)*@(example|xmple|examp).(com|org|net) could be used filter based on a number of combinations of email domain names.

Action

- **Mark as Spam**
  If this is the selected action, the email will be allowed through but it will be tagged with an indicator that clearly marks the email as spam.
- **Mark as Clear**
  If this is the selected action, the email will be allowed to go through to its destination on the assumption that the message is not spam.
- **Mark as Reject**
  If this is the selected action, the email will be dropped at the before reaching its destination.

Status

Indicates whether this particular list is enabled or disabled

Banned word check

When you enable banned word checking, your FortiGate unit will examine the email message for words appearing in the banned word list specified in the email filter profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the email filter profile, your FortiGate unit will treat the message as spam.

When determining the banned word score total for an email message, each banned word score is added once no matter how many times the word appears in the message. Use the command `config spamfilter bword` to add an email banned word list. Use the command `config spamfilter profile` to add a banned word list to an email filtering profile.

How content is evaluated

Every time the banned word filter detects a pattern in an email message, it adds the pattern score to the sum of scores for the message. You set this score when you create a new pattern to block content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the total score equals or exceeds the threshold, the email message is considered as spam and treated according to the spam action configured in the email filter profile. The score for each pattern is counted only once, even if that pattern appears many times in the email message. The default score for banned word patterns is 10 and the default threshold is 10. This means that by default, an email message is blocked by a single match.

A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.

For example, the FortiGate unit scans an email message that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the email message.”

Banned word pattern	Pattern type	Assigned score	Score added to the sum for the entire page	Comment
word	Wildcard	20	20	The pattern appears twice but multiple occurrences are only counted once.
word phrase	Wildcard	20	0	Although each word in the phrase appears in the message, the words do not appear together as they do in the pattern. There are no matches.
word*phrase	Wildcard	20	20	The wildcard represents any number of any character. A match occurs as long as “word” appears before “phrase” regardless of what is in between them.
mail*age	Wildcard	20	20	Since the wildcard character can represent any characters, this pattern is a match because “email message” appears in the message.

In this example, the message is treated as spam if the banned word threshold is set to 60 or less.

Adding words to a banned word list

When you enter a word, set the `Pattern-type` to wildcards or regular expressions.

Wildcard uses an asterisk (“*”) to match any number of any character. For example, re* will match all words starting with “re”.

Regular expression uses Perl regular expression syntax. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.

DNS-based Blackhole List (DNSBL)

A DNSBL is a list of IP addresses, usually maintained by a third party, which are identified as being associated with spamming.

FortiGuard-Antispam Service.

FortiGuard IP address check

The FortiGate unit queries the FortiGuard Antispam Service to determine if the IP address of the client delivering the email is blacklisted. A match will cause the FortiGate unit to treat delivered messages as spam.

The default setting of the `smtp-spamhdrip` CLI command is `disable`. When you enable FortiGuard IP address checking, your FortiGate unit will submit the IP address of the client to the FortiGuard service for checking. If the IP address exists in the FortiGuard IP address black list, your FortiGate unit will treat the message as spam.

FortiGuard URL check

When you enable FortiGuard URL checking, your FortiGate unit will submit all URLs appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL black list, your FortiGate unit will treat the message as spam.

FortiGuard email checksum check

When you enable FortiGuard email checksum checking, your FortiGate unit will submit a checksum of each email message to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum black list, your FortiGate unit will treat the message as spam.

Detect phishing URLs in email

When you enable FortiGuard phishing URL detection, your FortiGate unit will submit all URL hyperlinks appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL phishing list, your FortiGate unit will remove the hyperlink from the message. The URL will remain in place, but it will no longer be a selectable hyperlink.

FortiGuard spam submission

Spam submission is a way you can inform the FortiGuard AntiSpam service of non-spam messages incorrectly marked as spam. When you enable this setting, the FortiGate unit adds a link to the end of every message marked as spam. You then select this link to inform the FortiGuard AntiSpam service when a message is incorrectly marked.

Trusted IP Addresses

A list if IP addresses that are trusted by the FortiGate is created. Any email traffic coming in from these IP address will be exempted to perform IP based check, such as DNSBL/RBL, FortiShield SPAM IP or locally defined IP black list check.

If the FortiGate unit sits behind a company's Mail Transfer Units, it may be unnecessary to check email IP addresses because they are internal and trusted. The only IP addresses that need to be checked are those from outside of the company. In some cases, external IP addresses may be added to the list if it is known that they are not sources of spam.

MIME header

This feature filters by the MIME header. MIME header settings are configured in a separate part of the command tree but MIME header filtering is enabled within each profile.

HELO DNS lookup

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. The FortiGate unit takes the domain name specified by the client in the HELO and does a DNS lookup to determine if the domain exists. If the lookup fails, the FortiGate unit determines that any messages delivered during the SMTP session are spam.

The HELO DNS lookup is available only for SMTP traffic.

Return email DNS check

The FortiGate unit performs a DNS lookup on the If no such record exists, the message is treated as spam.

When you enable return email DNS checking, your FortiGate unit will take the domain in the reply-to email address and reply-to domain and check the DNS servers to see if there is an A or MX record for the domain. If the domain does not exist, your FortiGate unit will treat the message as spam.

Order of spam filtering

The FortiGate unit checks for spam using various filtering techniques. The order in which the FortiGate unit uses these filters depends on the mail protocol used.

Filters requiring a query to a server and a reply (FortiGuard Antispam Service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each spam filter passes the email to the next if no matches or problems are found. If the action in the filter is **Mark as Spam**, the FortiGate unit tags the email as spam according to the settings in the email filter profile.

For SMTP and SMTPS, if the action is discard, the email message is discarded or dropped.

If the action in the filter is **Mark as Clear**, the email is exempt from any remaining filters. If the action in the filter is **Mark as Reject**, the email session is dropped. Rejected SMTP or SMTPS email messages are substituted with a configurable replacement message.

Order of SMTP and SMTPS spam filtering

The FortiGate unit scans SMTP and SMTPS email for spam in the order given below. SMTPS spam filtering is available on FortiGate units that support SSL content scanning and inspection.

1. IP address black/white list (BWL) check on last hop IP
2. DNSBL & ORDBL check on last hop IP, FortiGuard Antispam IP check on last hop IP, HELO DNS lookup
3. MIME headers check, E-mail address BWL check
4. Banned word check on email subject
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Banned word check on email body
7. Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check on public IP extracted from header.

Order of IMAP, POP3, IMAPS and POP3S spam filtering

The FortiGate unit scans IMAP, POP3, IMAPS and POP3S email for spam in the order given below. IMAPS and POP3S spam filtering is available on FortiGate units that support SSL content scanning and inspection.

1. MIME headers check, E-mail address BWL check
2. Banned word check on email subject
3. IP BWL check
4. Banned word check on email body
5. Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check.

Spam actions

When spam is detected, the FortiGate unit will deal with it according to the **Spam Action** setting in the email filter profile. Note that POP3S, IMAPS and SMTPS spam filtering is available only on FortiGate units that support SSL content scanning and inspection. POP3, IMAP, POP3S and IMAPS mail can only be tagged. SMTP and SMTPS mail can be set to **Discard** or **Tagged**:

Discard

When the spam action is set to **Discard**, messages detected as spam are deleted. No notification is sent to the sender or recipient.

Pass

When the spam action is set to pass, message the spam filter is disabled for this message.

Tag

When the spam action is set to **Tagged**, messages detected as spam are labelled and delivered normally. The text used for the label is set in the **Tag Format** field and the label is placed in the subject or the message header, as set with the **Tag Location** option.

Email traffic types to inspect

The FortiGate unit examines IMAP, POP3, and SMTP email traffic. If your FortiGate unit supports content inspection, it can also examine IMAPS, POP3S, and SMTPS traffic. The options that you will see in the profile window are IMAP, POP3 and SMTP.

Configuring an Email Filters

FortiGuard email filtering techniques us FortiGuard services to detect the presence of spam among your email. A FortiGuard subscription is required to use the FortiGuard email filters. To enable email filtering an email filter needs to be created and then the filter needs to be associated with a security policy.

The filter can be created as follows:

- Go to Security **Profiles > Email Filter**.
  - Select the Create New icon (a plus symbol in a circle in the upper right hand corner).
  - Select the List icon (a page symbol in the upper right hand corner) and in the new window select **Create New**.

An existing filter can be edited as follows:

- Go to Security **Profiles > Email Filter**.
  - Select the filter that you wish to edit from the dropdown menu in the upper right corner.
  - Select the List icon (a page symbol in the upper right hand corner) and select the filter that you wish to edit from the list.

Once you are in the proper **Edit Email Filter Profile** window, you can enter a name in the Name field if it's a new filter.

The Comments field is for a discription or other information that will assist in understanding the function or purpose of the this particular filter.

Using the radio buttons for the Inspection Mode field, select either Proxy or Flow-based.

Before any of the other features or options of the filter appear the checkbox next to Enable Spam Detection and Filtering must be checked.

Spam detection by protocol

This matrix includes 3 rows that represent the email protocols IMAP, POP3 and SMTP.

There are also columns for:

Spam Action

For the client protocols, IMAP and POP3 the options are:

- **Tag** - This action will insert a tag into the email somewhere so that when the recipients view the email they will be warned that it is likely a spam.
- **Pass** - This action will allowany emails marked as spam to pass through without change. If this option is chosen, the Tag comments will be greyed out.

For the tranfer protocol, SMTP, the options are:

- **Tag** - This action will insert a tag into the email somewhere so that when the recipients view the email they will be warned that it is likely a spam.
- **Discard** - The action will drop the email before it reaches its destination.
- **Pass** - This action will allowany emails marked as spam to pass through without change. If this option is chosen, the Tag comments will be greyed out.

Tag Location

- **Subject** - The contents of the Tag Format will be inserted into the subject line. The subject line is the most commonly used.
- **MIME** - The contents of the Tag Format will be insterted in with the MIME header header.

Tag Format

The contents of this field will be entered into the tag location specified. The most common tag is something along the lines of [Spam] or **SPAM**

FortiGuard Spam Filtering

The options in the section are ones that require a FortiGuard subscription.

The options available in this section, to be selected by checkbox are:

- IP Address Check
- URL Check
- Detect Phishing URLs in Email
- Email Checksum Check
- Spam Submission

Local Spam Filtering

The options in the section are ones can be managed on the local device without the need for a FortiGuard subscription.

The options available in this section, to be selected by checkbox are:

- HELO DNS Lookup
- Return Email DNS Check
- Black White List - checking this option will produce a table that can be edited to create a number of BWL lists that can be separately configured and enabled.

Email filter examples

Configuring simple antispam protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antispam protection on a FortiGate unit located in a satellite office.

Creating an email filter profile

Most email filter settings are configured in an email filter profile. Email filter profiles are selected in firewall policies. This way, you can create multiple email filter profiles, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one email filter profile.

To create an email filter profile — web-based manager

1. Go to **Security Profiles > Email Filter**.
2. Select the **Create New** icon in the Edit Email Filter Profile window title.
3. In the **Name** field, enter `basic_emailfilter`.
4. Select **Enable Spam Detection and Filtering**.
5. Ensure that **IMAP**, **POP3**, and **SMTP** are selected in the header row.

   These header row selections enable or disable examination of each email traffic type. When disabled, the email traffic of that type is ignored by the FortiGate unit and no email filtering options are available.
6. Under **FortiGuard Spam Filtering**, enable **IP Address Check**.
7. Under **FortiGuard Spam Filtering**, enable **URL Check**.
8. Under **FortiGuard Spam Filtering**, enable **E-mail Checksum Check**.
9. Select **OK** to save the email filter profile.

To create an email filter profile — CLI

```
config spamfilter profile
   edit basic_emailfilter
      set options spamfsip spamfsurl spamfschksum
   end
```

Selecting the email filter profile in a security policy

An email filter profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an email filter profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the email filter profile in a security policy — web-based manager

1. Go to **Policy > Policy > IPv4.**
2. Create a new or edit a policy.
3. Turn on email filtering.
4. Select the `basic_emailfilter` profile from the list.
5. Select **OK** to save the security policy.

To select the email filter profile in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set profile-protocol-options default
      set spamfilter-profile basic_emailfilter
   end
```

IMAP, POP3, and SMTP email traffic handled by the security policy you modified will be scanned for spam. Spam messages have the text “Spam” added to their subject lines. A small office may have only one security policy configured. If you have multiple policies, consider enabling spam scanning for all of them.

Blocking email from a user

Employees of the Example.com corporation have been receiving unwanted email messages from a former client at a company called example.net. The client’s email address is client@example.net. All ties between the company and the client have been severed, but the messages continue. The FortiGate unit can be configured to prevent these messages from being delivered.

To enable Email Filter

1. Go to **Security Profiles > Email Filter > Profile**.
2. Select the email filter profile that is used by the firewall policies handling email traffic from the email filter profile drop down list.
3. In the row **Tag Location**, select **Subject** for all three mail protocols.
4. In the row **Tag Format**, enter `SPAM:` in all three fields.
   This means that normal spam will be tagged in the subject line.
5. Select **Enable Spam Detection and Filtering**.
6. Under **Local Spam Filtering**, enable **Black White List** and select **Create New**.
7. In the Black White List widget, select **Create New**.

8. Select **Email Address Wildcard**.
9. Enter `client@example.net` in the **Pattern** field.
   - If you wanted to prevent everyone's email from the client's company from getting through you could have used *@example.net instead.
10. Set the **Action** as **Mark as Spam**.
11. Set the **Status** to **Enable**.
12. Confirm that the SMTP protocol action is set to **Discard**.
13. Select **OK**.

Now that the email address list is created, you must enable the email filter in the email filter profile.

When this email filter profile is selected in a security policy, the FortiGate unit will reject any email message from an address ending with @example.net for all email traffic handled by the security policy.

Data leak prevention

The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through the FortiGate unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the FortiGate unit.

This section describes how to configure the DLP settings.

The following topics are included:

- Data leak prevention concepts
- Enable data leak prevention
- Fingerprint
- File filter
- DLP archiving
- DLP examples

Log Only is enabled by default.

Data leak prevention concepts

Data leak prevention examines network traffic for data patterns you specify. You define whatever patterns you want the FortiGate unit to look for in network traffic. The DLP feature is broken down into a number of parts.

DLP sensor

A DLP sensor is a package of filters. To use DLP, you must enable it in a security policy and select the DLP sensor to use. The traffic controlled by the security policy will be searched for the patterns defined in the filters contained in the DLP sensor. Matching traffic will be passed or blocked according to how you configured the filters.

DLP filter

Each DLP sensor has one or more filters configured within it. Filters can examine traffic for known files using DLP fingerprints, for files of a particular type or name, for files larger than a specified size, for data matching a specified regular expression, or for traffic matching an advanced rule or compound rule.

You can configure the action taken when a match is detected. The actions include:

- None
- Log Only
- Block
- Quarantine IP address

Log Only is enabled by default.

DLP Filter Actions

None

No action is taken if filter even if filter is triggered

Log Only

The FortiGate unit will take no action on network traffic matching a rule with this action. The filter match is logged, however. Other matching filters in the same sensor may still operate on matching traffic.

Block

Traffic matching a filter with the block action will not be delivered. The matching message or download is replaced with the data leak prevention replacement message.

Quarantine IP Address/ Source IP ban

Starting in FortiOS 5.2, the quarantine, as a place where traffic content was held in storage where it couldn't interact with the network or system was removed, but the term quarantine was kept to describe keeping selected source IPs from interacting with the network and protected systems. This source IP ban is kept in the kernel rather than in any specific application engine and can be queried by APIs. The features that can use the APIs to access and use the banned source IP addresses are antivirus, DLP, DoS and IPS. Both IPv4 and IPv6 version are included in this feature.

If the **quarantine-ip** action is used, the additional variable of expiry time will become available. This variable determines for how long the source IP adddress will be blocked. In the GUI it is shown as a field before minutes. In the CLI the option is called `expiry` and the duration is in the format `<###d##h##m>`. The maximum days value is 364. The maximum hour value is 23 and the maximum minute value is 59. The default is 5 minutes.

Configure using the CLI

To configure the DLP sensor to add the source IP address of the sender of a protected file to the quarantine or list of banned source IP addresses edit the DLP Filter, in the CLI. as follows:

```
config dlp sensor
   edit <sensor name>
      config filter
         edit <id number of filter>
            set action quarantine-ip
            set expiry 5m
            end
         end
```

Preconfigured sensors

A number of preconfigured sensors are provided with your FortiGate unit. These can be edited or added to more closely match your needs.

Some of the preconfigured sensors with filters ready to go are:

- Credit-Card - This sensor logs the traffic, both files and messages, that contain credit card numbers in the formates used by American Express, MasterCard and Visa.

- SSN-Sensor - This sensor logs the traffic, both files and messages, that contain Social Security Numbers with the exception of those that are WebEx invitation emails.

These rules affect only unencrypted traffic types. If you are using a FortiGate unit that can decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.

Before using the rules, examine them closely to ensure you understand how they will affect the traffic on your network.

DLP document fingerprinting

One of the DLP techniques to detect sensitive data is fingerprinting (also called document fingerprinting). Most DLP techniques rely on you providing a characteristic of the file you want to detect, whether it's the file type, the file name, or part of the file contents. Fingerprinting is different in that you provide the file itself. The FortiGate unit then generates a checksum fingerprint and stores it. The FortiGate unit generates a fingerprint for all files detected in network traffic, and it is compared to all of the fingerprints stored in its fingerprint database. If a match is found, the configured action is taken.

The document fingerprint feature requires a FortiGate unit with internal storage. The document fingerprinting menu item does not appear on models without internal storage.

Any type of file can be detected by DLP fingerprinting and fingerprints can be saved for each revision of your files as they are updated.

To use fingerprinting you select the documents to be fingerprinted and then add fingerprinting filters to DLP sensors and add the sensors to firewall policies that accept the traffic to which to apply fingerprinting.

Fingerprinting

Fingerprint scanning allows you to create a library of files for the FortiGate unit to examine. It will create checksum fingerprints so each file can be easily identified. Then, when files appear in network traffic, the FortiGate will generate a checksum fingerprint and compare it to those in the fingerprint database. A match triggers the configured action.

You must configure a document source or uploaded documents to the FortiGate unit for fingerprint scanning to work.

Fingerprinted Documents

The FortiGate unit must have access to the documents for which it generates fingerprints. One method is to manually upload documents to be fingerprinted directly to the FortiGate unit. The other is to allow the FortiGate unit to access a network share that contains the documents to be fingerprinted.

If only a few documents are to be fingerprinted, a manual upload may be the easiest solution. If many documents require fingerprinting, or if the fingerprinted documents are frequently revised, using a network share makes user access easier to manage.

Fingerprinting by document source

To configure a fingerprint document source

1. Go to **Security Profiles > Advanced > DLP Fingerprint**.
2. In the Document Sources section, select **Create New**.
3. Configure the settings:

Name	Enter a descriptive name for the document source.
Server Type	This refers to the type of server share that is being accessed. The default is Windows Share but this will also work on Samba shares.
Server Address	Enter the IP address of the server.
User Name	Enter the user name of the account the FortiGate unit uses to access the server network share.
Password	Enter the password for the account being used to access the network share.
Path	Enter the path to the document folder.
Filename Pattern	You may enter a filename pattern to restrict fingerprinting to only those files that match the pattern. To fingerprint all files, enter an asterisk (“*”).
Sensitivity Level	Select a sensitivity level. The sensitivity is a tag for your reference that is included in the log files. It does not change how fingerprinting works.
Scan Periodically	To have the files on the document source scanned on a regular basis, select this option. This is useful if files are added or changed regularly. Once selected, you can choose Daily, Weekly, or Monthly update options.The Hour and Min fields are for determining, in a 24 hour clock, the time that the source shares will be scanned.
Advanced	Expand the Advanced heading for additional options.
Fingerprint files in sub-directories	By default, only the files in the specified path are fingerprinted. Files in sub-directories are ignored. Select this option to fingerprint files in sub-directories of the specified path.
Remove fingerprints for deleted files	Select this option to retain the fingerprints of files deleted from the document source. If this option is disabled, fingerprints for deleted files will be removed when the document source is rescanned.
Keep previous fingerprints for modified files	Select this option to retain the fingerprints of previous revisions of updated files. If this option is disabled, fingerprints for previous version of files will be deleted when a new fingerprint is generated.

4. Select **OK**.

Fingerprinting manually by document

To configure manual document fingerprints

1. Go to **Security Profiles > Advanced > DLP Fingerprint**.
2. In the Manual Document Fingerprints section, select **Create New**.

3. Use the Browse feature for the File field to select the file to be fingerprinted. The selection will be limited to network resourses
4. Choose a Sensitivity level. The default choices are **Critical**, **Private** and **Warning**, but more can be added in the CLI.
5. If the file is an archive containing other files, select **Process files inside archive** if you also want the individual files inside the archive to have fingerprints generated in addition to the archive itself.
6. Select **OK**.
   The file is uploaded and a fingerprint generated.

File size

This filter-type checks for files exceeding a configured size. All files larger than the specified size are subject to the configured action. The value of the field is measured in Kilobytes.

DLP filtering by specific file types

File filters use file filter lists to examine network traffic for files that match either file names or file types. For example, you can create a file filter list that will find files called secret.* and also all JPEG graphic files. You can create multiple file filter lists and use them in filters in multiple DLP sensors as required.

Specify File Types is a DLP option that allows you to block files based on their file name or their type.

- **File types** are a means of filtering based on an examination of the file contents, regardless of the file name. If you block the file type **Archive (zip)**, all zip archives are blocked even if they are renamed with a different file extension. The FortiGate examines the file contents to determine what type of file it is and then acts accordingly.
- **File Name patterns** are a means of filtering based purely on the names of files. They may include wildcards (*). For example, blocking *.scr will stop all files with an scr file extension, which is commonly used for Windows screen saver files. Files trying to pass themselves off as Windows screen saver files by adopting the file-naming convention will also be stopped.
  - Files can specify the full or partial file name, the full or partial file extension, or any combination. File pattern entries are not case sensitive. For example, adding `*.exe` to the file pattern list also blocks any files ending with `.EXE`.
  - Files are compared to the enabled file patterns from top to bottom, in list order.

File filter detects files within archives for FortiOS 5.0.8, 5.2.0 and later. If you set the file type as `*.txt`, for example, text files inside of zip files will be detected.

Watermarking

Watermarking is essentially marking files with a digital pattern to mark the file as being proprietary to a specific company. Fortinet has a utility that will apply a digital watermark to files. The utility adds a small (approx. 100 byte) pattern to the file that is recognised by the DLP Watermark filter. the pattern is invisible to the end user.

When watermarking a file it should be verified that the pattern matches up to a category found on the FortiGate firewall. For example, if you are going to watermark a file with the sensitivity level of “Secret” you should verify that “Secret” is a sensitivity level that has been assigned in the FortiGate unit.

Watermark Sensitivity

If you are using watermarking on your files you can use this filter to check for watermarks that correspond to sensitivity categories that you have set up.

The Corporate Identifier is to make sure that you are only blocking watermarks that your company has place on the files, not watermarks with the same name by other companies.

Software Versions

Before planning on using watermarking software it is always best to verify that the software will work with your OS. Currently, the only utility available to watermark files is within the FortiExplorer software and that is only only available for the Windows operating system. There was an older version of software that is for Linux and is Commandline only, but is has been discontinued.

File types

The Watermark tool does not work with every file type. The following file types are supported by the watermark tool:

- .txt
- .pdf
- .doc
- .xls
- .ppt
- .docx
- .pptx
- .xlsx

Currently the DLP only works with Fortinet's watermarking software.

Using the FortiExplorer Watermark tool

The FortiExplorer software can be downloaded from the Fortinet Support Site.

1. Choose whether to "Apply Watermark To:"
   - Select File
   - Entire Directory
2. Fill in the fields:
   a. **Select File**
   This Field has a browse icon next to it which will allow the user to browse to and select a single file or directory to apply the water mark to.
   b. **Sensitivity Level**
   This field is a drop down menu that lists the available sensitivity levels that the FortiGate can scan for
   c. **Identifier**
   This is a unique identifier string of characters to identify the company that the document belongs to.
   d. **Output Directory**
   This Field has a browse icon next to it which will allow the user to browse to a directory where the altered file

will be placed. If the output directory is the same as the source directory the original file will be overwritten. If the output directory is different than the source directory then the watermarked version of the file will be place there and the unaltered original will be left in the source directory.

3. Select **Apply Watermark** to start the process.

Regular expression

The FortiGate unit checks network traffic for the regular expression specified in a regular expression filter. The regular expression library used by Fortinet is a variation of a library called PCRE (Perl Compatible Regular Expressions). A number of these filters can be added to a sensor making a sort of 'dictionary' subset within the sensor.

Some other, more limited DLP implementations, use a list of words in a text file to define what words are searched for. While the format used here is slightly different than what some people are used to, the resulting effect is similar. Each Regular Expression filter can be thought of as a more versatile word to be searched against. In this dictionary (or sensor), the list of words is not limited to just predefined words. It can include expressions that can accommodate complex variations on those words and even target phrases. Another advantage of the individual filter model of this dictionary over the list is that each word can be assigned its own action, making this implementation much more granular.

Encrypted

This filter is a binary one. If the file going through the policy is encrypted the action is triggered.

Examining specific services

To assist in optimizing the performance of the firewall, the option exists to select which services/protocol traffic will be checked for the targeted content.This setting gives you a tool to save the resources of the FortiGate unit by only using processing cycles on the relevant traffic. Just check the boxes associated with the service / protocol that you want to have checked for filter triggers.

DLP archiving

DLP is typically used to prevent sensitive information from getting out of your company network, but it can also be used to record network use. This is called DLP archiving. The DLP engine examines email, FTP, NNTP, and web traffic. Enabling archiving for rules when you add them to sensors directs the FortiGate unit to record all occurrences of these traffic types when they are detected by the sensor.

Since the archive setting is configured for each rule in a sensor, you can have a single sensor that archives only the things you want.

You can archive Email, FTP, HTTP, and session control content:

- Email content includes IMAP, POP3, and SMTP sessions. Email content can also include email messages tagged as spam by Email filtering. If your unit supports SSL content scanning and inspection, Email content can also include IMAPS, POP3S, and SMTPS sessions.
- HTTP content includes HTTP sessions. If your unit supports SSL content scanning and inspection HTTP content can also include HTTPS sessions.

DLP archiving comes in two forms: **Summary Only**, and **Full**.

Summary archiving records information about the supported traffic types. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses the Web, every URL the user visits recorded. The result is a summary of all activity the sensor detected.

For more detailed records, full archiving is necessary. When an email message is detected, the message itself, including any attachments, is archived. When a user accesses the Web, every page the user visits is archived. Far more detailed than a summary, full DLP archives require more storage space and processing.

Because both types of DLP archiving require additional resources, DLP archives are saved to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service (subscription required).

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the Fortinet configuration. The FortiGuard Analysis server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

Two sample DLP sensors are provided with DLP archiving capabilities enabled. If you select the `Content_Summary` sensor in a security policy, it will save a summary DLP archive of all traffic the security policy handles. Similarly, the `Content_Archive` sensor will save a full DLP archive of all traffic handled the security policy you apply it to. These two sensors are configured to detect all traffic of the supported types and archive them.

DLP archiving is set in the CLI only.

To set the archive to Full

```
config dlp sensor
   edit <name of sensor>
      set full-archive-proto smtp pop3 imap http ftp nntp msn yahoo mapi
   end
```

To set the archive to Summary Only

```
config dlp sensor
   edit <name of sensor>
      set summary-proto smtp pop3 imap http ftp nntp msn yahoo mapi
   end
```

Enable data leak prevention

DLP examines your network traffic for data patterns you specify. The FortiGate unit then performs an action based on the which pattern is found and a configuration set for each filter trigger.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a DLP sensor.
   New DLP sensors are empty. You must create one or more filters in a sensor before it can examine network traffic.
2. Add one or more filters to the DLP sensor.
   Each filter searches for a specific data pattern. When a pattern in the active DLP sensor appears in the traffic, the FortiGate unit takes the action configured in the matching filter. Because the order of filters within a sensor cannot be changed, you must configure DLP in sequence.
3. Add the DLP sensor to one or more firewall policies that control the traffic to be examined.

Creating/editing a DLP sensor

DLP sensors are collections of filters. You must also specify an action for the filter when you create it in a sensor. Once a DLP sensor is configured, you can select it a security policy profile. Any traffic handled by the security policy will be examined according to the DLP sensor configuration.

To create/edit a DLP sensor

1. Go to **Security Profiles > Data Leak Prevention**.
2. Choose whether you want to edit an exiting sensor or create a new one.
   - The default sensor will be the one displayed by default.
   - If you are going to edit an existing sensor, selecting it can be done by either using the drop down menu in the upper right hand corner of the window or by selecting the List icon (the furthest right of the 3 icons in the upper right of the window, if resembles a page with some lines on it), and then selecting the profile you want to edit from the list.
   - If you need to create a new sensor you can either select the Create New icon (a plus sign within a circle) or select the List icon and then select the Create New link in the upper left of the window that appears.
3. Enter a name in the **Name** field for any new DLP sensors.
4. Optionally, you may also enter a comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.
5. At this point you can add filters to the sensor (see adding filters to a DLP sensor) or select **OK** to save the sensor.

Without filters, the DLP sensor will do nothing.

Adding filters to a DLP sensor

Once you have created a DLP sensor, you need to add filters.

1. To add filters to a DLP sensor
2. Go to **Security Profiles > Data Leak Prevention**.
3. Select the Sensor you wish to edit using the drop down menu or the sensor list window.
4. Within the Edit DLP Sensor window select **Create New**. A New Filter window should pop up.
5. Select the type of filter. You can choose either Messages or Files. Depending on which of these two are chosen different options will be available.

   Message filter will have these configuration options:
   - [radio button] Containing: [drop down menu including: Credit Card # or SSN]
   - [radio button] Regular Expression [input field]

   Examine the following Services:

   Web Access

   - HTTP-POST

   Email

   - [check box] SMTP
   - [check box] POP3
   - [check box] IMAP
   - [check box] MAPI

Others

- [check box] NNTP

Action [from drop down menu]

- None
- Log Only,
- Block
- Quarantine IP address

Files filter will have these options:

- [radio button] Containing: drop down menu including: Credit Card # or SSN
- [radio button] File Size >= [ ]KB
- [radio button] Specify File Types
  File Types: ["Click to add…"drop down menu of File extensions]
  File Name Patterns:["Click to add…"drop down menu]
- [radio button] File Finger Print : [drop down menu]
- [radio button] Watermark Sensitivity: [drop down menu] and Corporate Identifier [id field]
- [radio button] Regular Expression [input field]
- [radio button] Encrypted

Examine the following Services:

Web Access

- [check box] HTTP-POST
- [check box] HTTP-GET

Email

- [check box] SMTP
- [check box] POP3
- [check box] IMAP
- [check box] MAPI

Others

- [check box] FTP
- [check box] NNTP

Action [from drop down menu]

- None
- Log Only,
- Block
- Quarantine IP address

6. Select **OK**.
7. Repeat Steps 6 and 7 for each filter.
8. Select **Apply** to confirm the settings of the sensor.

If you have configured DLP to block IP addresses and if the FortiGate unit receives sessions that have passed through a NAT device, all traffic from that NAT device — not just traffic from individual users — could be blocked. You can avoid this problem by implementing authentication.

To view or modify the replacement message text, go to **System > Config > Replacement Message**.

DLP examples

Blocking content with credit card numbers

When the objective is to block credit card numbers one of the important things to remember is that 2 filters will need to be used in the sensor.

In the default Credit-Card sensor, you will notice a few things.

- The Action is set to Log Only
- In the Files filter not all of the services are being examined.

If you wish to block as much content as possible with credit card numbers in it instead of just logging most the traffic that has it, the existing sensor will have to be edited.

1. **Go to Security Profile** > **Data Leak Prevention**

Some configurations will have a preconfigured Credit Card sensor where you can use the drop down menu to select **Credit-Card**. If your configuration doesn't already have one create a new sensor.

2. Use the **Create New** icon to add a new sensor.
3. Create/edit the first filter. Use the following settings:
   Filter

Filter	Messages
Filter option	Credit Card #

   Examine the Following Services

   Make sure all of the services are being examined.

   Action

   Set action to **Block**.

   Select **OK** or **Apply**.

4. Create/edit the first filter. Use the following settings:
   Filter

Filter	Files
Filter option	Credit Card #

Examine the Following Services

Make sure all of the services are being examined.

Action

Set action to **Block**.

Select OK or Apply

5. Edit the appropriate policies so that under **Security Profiles**, **DLP** is turned on and the **Credit-Card** sensor is selected.

Blocking emails larger than 15 MB and logging emails from 5 MB to 15 MB

Multiple filters will have to be used in this case and the order that they are used is important. Because there is no mechanism to move the filters within the sensor the order that they are added to the sensor is important.

1. **Go to Security Profile** > **Data Leak Prevention.**
2. Use the **Create New** icon to add a new sensor.
   Use the following values:

Name	large_emails
Comment	<optional>

Once the Sensor has been created, a new filter will need to be added.

3. Create the filter to block the emails over 15 MB. In the filters table select **Create New**.
   Use the following values:
   Filter

Filter	Messages
Filter option	File Size >=
KB	15360 (1MB = 1024KB, 15 MB = 15 x 1024KB = 15360KB)

Examine the Following Services

Make sure all of the Email services are being examined.

Action

Set action to **Block**.

Select **OK**.

4. Create the filter to log emails between 5 MB and 10 MB. In the filters table select **Create New**.
   Use the following values
   Filter

Filter	Messages
Filter option	File Size >=
KB	5120 (1MB = 1024KB, 5 MB = 5 x 1024KB = 5124 KB)

Examine the Following Services

Make sure all of the Email services are being examined.

Action

Set action to **Block**.

Select **OK**.

The reason that the block filter is placed first is because the filters are applied in sequence and once the traffic triggers a filter the action is applied and then the traffic is passed on to the next test. If the Log Only filter which checks for anything over 1MB is triggered this would include traffic over 15MB, so a 16 MB file would only be logged. In the described order, the 16 MB file will be blocked and the 3 MB file will be logged.

Selective blocking based on a finger print

The following is a fairly complex example but shows what can be done by combining various components in the correct configuration.

The company has a number of copyrighted documents that it does not want “escaping” to the Internet but it does want to be able to send those documents to the printers for turning into hardcopy.

The policies and procedures regarding this issue state that:

- Only members of the group **Senior_Editors** can send copyrighted material to the printers.
- Every member of the company by default is included in the group **employees**.
- Even permitted transmission of copyrighted material should be recorded.
- All of the printers IP addresses are in a group called **approved_printers**.
- There is a file share called copyrighted where any file that is copyrighted is required to have a copy stored.
- It doesn’t happen often but for legal reasons sometimes these files can be changed, but all versions of a file in this directory need to be secured.
- All network connections to the Internet must have Antivirus enabled using at least the default profile.
- The SSL/SSH Inspection profile used will be **default**.

It is assumed for the purposes of this example that:

- Any addresses or address groups have been created.
- User accounts and groups have been created.
- The account used by the FortiGate is fgtaccess.
- The copyrighted sensitivity level needs to be created.
- The copyrighted material is stored at \\192.168.27.50\books\copyrighted\

1. Add a new Sensitivity Level by running the following commands in the CLI

```
config dlp fp-sensitivity
   edit copyrighted
end
```

2. Apply files to the fingerprint database

a. Go to **Security Profiles** > **Advanced** > **DLP Fingerprint**.

b. In the **Document Sources** section **select Create New**.
Use the following field values:

Name	copyrighted_material
Server Type	Windows Share
Server Address	192.168.27.50
User Name	fgtaccess
Password	******
Path	books/copyrighted/
Filename Pattern	*.pdf
Sensitivity	copyrighted
Scan Periodically	enabled
<Frequency>	Daily, Hour: 2, Min: 0
Advanced	
Fingerprint files in sub-directories	enabled
Remove fingerprints for deleted files	not enabled
Keep previous fingerprints for modified files	enabled

Two Sensors need to be created. One for blocking the transmission of copyrighted material and a second for allowing the passing of copyrighted material under specific circumstances.

3. Create the first DLP Sensor
   - Go to **Security Profile** > **Data Leak Prevention**.
   - Create a new sensor.
     Use the following field values:

Name	block_copyrighted
Comment	<optional>

   - In the Filter table, select **Create New**.
     Use the following values

     Filter

Filter	Files
Filter option	File Finger Print
Finger print value from dropdown	“copyrighted”

Examine the Following Services

Make sure all of the services are being examined.

Action

From the drop down menu choose **Block**

4. Create the second DLP Sensor
   - Go to **Security Profile** > **Data Leak Prevention**.
   - Create a new sensor.
     Use the following field values:

Name	allow_copyrighted
Comment	<optional>

   - In the Filter table, select **Create New**.
     Use the following values

     Filter

Filter	Files
Filter option	File Finger Print
Finger print value from dropdown	“copyrighted”

Examine the Following Services

Make sure all of the services are being examined.

Action

From the drop down menu choose **Log Only**

5. Create a policy to allow transmission of copyrighted material.
   a. Go to **Policy & Objects > Policy > IPv4**.
   b. Select **Create New**.
   c. Use the following values in the Policy:

Incoming Interface	LAN

Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	all
Action	ACCEPT
Enable NAT	enabled -- Use Destination Interface Address
Antivirus	<ON> default
DLP	<ON> Copyrighted
SSL/SSH Inspection	<ON> default
Enable this policy	<ON>

This policy should be place as close to the beginning of the list of policies so the it is among the first tested against.

6. Create a policy to block transmission of copyrighted material.
This will in effect be the default template for all following policies in that they will have to use the DLP profile that blocks the transmission of the copyrighted material.
   a. Go to **Policy & Objects > Policy > IPv4**
   b. Select **Create New** or Edit an existing policy.
   c. Use the following values in the Policy:

   The fields should include what ever values you need to accomplish your requirements are but each policy should include the DLP sensor block_copyrighted or if a different DLP configuration is required it should include a filter that blocks **copyrighted** fingerprinted file.

   If you need to create a policy that is identity based make sure that there is an Authentication rule for the group **employees** that uses the DLP sensor that blocks copyrighted material.

ICAP

ICAP is the acronym for Internet Content Adaptation Protocol The purpose of the feature is to off load work that would normally take place on the firewall to a separate server specifically set up for the specialized processing of the incoming traffic. This takes some of the resource strain off of the FortiGate firewall leaving it to concentrate its resources on things that only it can do.

Off-loading value-added services from Web servers to ICAP servers allows those same web servers to be scaled according to raw HTTP throughput versus having to handle these extra tasks.

ICAP servers are focused on a specific function, for example:

- Ad insertion
- Virus scanning
- Content translation
- HTTP header or URL manipulation
- Language translation
- Content filtering

ICAP does not appear by default in the web-based manager. You must enable it in **System > Admin > Settings** to display ICAP in the web-based manager.

The following topics are included in this section:

- The Protocol
- Offloading using ICAP
- Configuration Settings
- Example ICAP sequence
- Example Scenerio

The Protocol

The protocol is a lightweight member of the TCP/IP suite of protocols. It is an Application layer protocol and its specifications are set out in RFC 3507. The default TCP that is assigned to it is 1344. Its purpose is to support HTTP content adaptation by providing simple object-based content vectoring for HTTP services. ICAP is usually used to implement virus scanning and content filters in transparent HTTP proxy caches. Content Adaptation refers to performing the particular value added service, or content manipulation, for an associated client request/response.

Essentially it allows an ICAP client, in this case the FortiGate firewall, to pass HTTP messages to an ICAP server like a remote procedure call for the purposes of some sort of transformation or other processing adaptation. Once the ICAP server has finished processing the the content, the modified content is sent back to the client.

The messages going back and forth between the client and server are typically HTTP requests or HTTP responses. While ICAP is a request/response protocol similar in semantics and usage to HTTP/1.1 it is not HTTP nor does it run over HTTP, as such it cannot be treated as if it were HTTP. For instance ICAP messages can not be forwarded by HTTP surrogates.

Offloading using ICAP

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to an ICAP server in the ICAP profile added to the policy. Responses from the ICAP server are returned to the FortiGate unit which forwards them to an HTTP client or server.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers.

If the FortiGate unit supports HTTPS inspection, HTTPS traffic intercepted by a policy that includes an ICAP profile is also offloaded to the ICAP server in the same way as HTTP traffic.

When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Configuration Settings

There are 2 sections where ICAP is configured:

Servers

Go to **Security Profiles > Advanced > ICAP Servers**

The available settings to be configured regarding the server are

- **Name**
- **IP Type** (in the GUI) or IP address version (in the CLI)
  The options for this field in the GUI are 2 radio buttons labelled “IPv4” and “IPv4”. In the CLI the approach is slightly different. There is a field “ip-version” that can be set to “4” or “6”.
- **IP Address**
  Depending on whether you’ve set the IP version to 4 or 6 will determine the format that the content of this field will be set into. In the GUI it looks like the same field with a different format but in the CLI it is actually 2 different fields named “ip-address” and ip6-address.
- **Port**
  1344 is default TCP port used for the ICAP traffic. The range can be from 1 to 65535.

Maximum Connections

This value refers to the maximum number of concurrent connections that can be made to the ICAP server. The default setting is 100. This setting can only be configured in the CLI.

The syntax is:

```
config icap server
   edit <icap_server_name>
      set max-connections <integer>
      end
```

Profiles

Name

Just like any other profile each of the ICAP profiles needs to be assigned a name.

Enable Request Processing

Enabling this setting allows the ICAP server to process request messages.

If enabled this setting will also require:

- **Server** - This is the name of the ICAP server. It is chosen from the drop down menu in the field. The servers are configure in the Security Profiles > ICAP > Server section.
- **Path** - This is the path on the server to the processing compent. For instance if the Windows share name was “Processes” and the directory within the share was “Content-Filter” the path would be “/Processes/Content-Filter/”
- **On Failure** - There are 2 options. You can choose by the use of radio buttons either **Error** or **Bypass**.

Enable Response Processing

Enabling this setting allows the ICAP server to process response messages.

If enabled this setting will also require:

- **Server** - This is the name of the ICAP server. It is chosen from the drop down menu in the field. The servers are configure in the Security Profiles > ICAP > Server section.
- **Path** - This is the path on the server to the processing compent. For instance if the Windows share name was “Processes” and the directory within the share was “Content-Filter” the path would be “/Processes/Content-Filter/”
- **On Failure** - There are 2 options. You can choose by the use of radio buttons either **Error** or **Bypass**.

Enable Streaming Media Bypass

Enabling this setting allows streaming media to ignore offloading to the ICAP server.

Example ICAP sequence

This example is for an ICAP server performing web URL filtering on HTTP requests

1. A user opens a web browser and sends an HTTP request to connect to a web server.
2. The FortiGate unit intercepts the HTTP request and forwards it to an ICAP server.
3. The ICAP server receives the request and determines if the request is for URL that should be blocked or allowed.
   - If the URL should be blocked the ICAP server sends a response to the FortiGate unit. The FortiGate unit returns this response to the user’s web browser. This response could be a message informing the user that their request was blocked.
   - If the URL should be allowed the ICAP server sends a request to the FortiGate unit. The FortiGate unit forwards the request to the web server that the user originally attempted to connect to.
   - When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Example Scenario

Information relavent to the following example:

- The ICAP server is designed to do proprietary content filtering specific to the organization so it will have to receive the messages and sent back appropriate responses.
- The content filter is a required security precaution so it if the message cannot be processed it is not allowed through.

- Resources on both the Fortigate and the ICAP server are considerable so the maximum connections setting will set at a double the default value to analyse the impact on performance.
- The ICAP server's IP address is 172.16.100. 55.
- The path to the processing component is "/proprietary_code/content-filter/".
- Streaming media is not something that the filter considers, but is allowed through the policy so processing it would be a waste of resources.
- The ICAP profile is to be added to an existing firewall policy.
- It is assumed that the display of the policies has already been configured to show the column "ID".

1. Enter the following to configure the ICAP server:

   Go to **Security Profiles** > **Advanced** > **ICAP Server**.
   Use the following values:

Name	content-filtration-server4
IP Type	IPv4
IP Address	172.16.100.55
Port	1344

   Use the CLI to set the max-connections value.

```
config icap server
   edit content-filtration-server4
      set max-connections 200
      end
```

2. Enter the following to configure the ICAP profile to then apply to a security policy:

   Use the following values:

Name	Prop-Content-Filtration
Enable Request Processing	enable
Server	content-filtration-server4
Path	/proprietary_code/content-filter/
On Failure	Error
Enable Response Processing	enable
Server	content-filtration-server4
Path	/proprietary_code/content-filter/
On Failure	Error
Enable Streaming Media Bypass	enable

3. Apply the ICAP profile to policy:

The purposes of this particular ICAP profile is to filter the content of the traffic coming through the firewall via policy ID#17.

a. Go to **Policy & Objects** > **Policy** > **IPv4.**
b. Open the existing policy ID# 17 for editing.
c. Go to the section **Security Profiles.**
d. Select the button next to **ICAP** so that it indicates that it's status is **ON**.
e. Select the field with the profile name and use the drop down menu to select **Prop-Content-Filtration.**
f. Select **OK**.

Other Security Profiles considerations

The following topics are included in this section:

- Security Profiles and Virtual domains (VDOMs)
- Conserve mode
- SSL content scanning and inspection
- Using wildcards and Perl regular expressions

Security Profiles and Virtual domains (VDOMs)

If you enable virtual domains (VDOMs) on your FortiGate unit, all Security Profiles configuration is limited to the VDOM in which you configure it.

While configuration is not shared, the various databases used by Security Profiles features are shared. The FortiGuard antivirus and IPS databases and database updates are shared. The FortiGuard web filter and spam filter features contact the FortiGuard distribution network and access the same information when checking email for spam and web site categories and classification.

Conserve mode

FortiGate units perform all Security Profiles processing in physical RAM. Since each model has a limited amount of memory, the Conserve mode is activated to avoid a situation where the device is using so much memory to scan files that it becomes unresponsive. When the Conserve mode is activated the Antivirus engine proxy will not accept anymore sessions until the FortiGate leaves Conserve mode. This not only effects the Antivirus function but the DLP function as well.

The AV proxy

Most content inspection the FortiGate unit performs requires that the files, email messages, URLs, and web pages be buffered and examined as a whole. The AV proxy performs this function, and because it may be buffering many files at the same time, it uses a significant amount of memory. Conserve mode is designed to prevent all the component features of the FortiGate unit from trying to use more memory than it has. Because the AV proxy uses so much memory, conserve mode effectively disables it in most circumstances. As a result, the content inspection features that use the AV proxy are also disabled in conserve mode.

All of the Security Profiles features use the AV proxy with the exception of IPS, application control, DoS as well as flow-based antivirus, DLP, and web filter scanning. These features continue to operate normally when the FortiGate unit enters conserve mode.

Conserve mode trigger mechanisms

There are two separate triggers for activating the Conserve mode in FortiOS:

The first mechanism is that the proxies used for scanning content track the amount of shared memory that is in use and when it passes a given threshold the proxy triggers conserve mode. This mechanism is only operational if the applicable proxies are running. In past versions AV proxies were always running regardless of whether or not an AV profile was part of the configuration. In FortiOS version 5.x this was changed so that AV proxies were only running if required by the presence of an AV profile in the configuration. Because SIP is handled in the same

proxy as the IM protocols and IM protocols require an AV proxy meant that, because starting in 5.2 the SIP ALG was enabled by default, the AV proxies were again always running.

FortiOS 5.2.3 changed this so that AV proxies were not needed unless there was an AV profile because the proxies used to scan SIP could also do Conserve mode checking. This does mean that if you want to avoid the proxy Conserve mode checking mechanism you will also have to disable the SIP ALG.

The second mechanism is that the kernel checks the amount of free memory on the system and if the amount of memory available for use drops below the given threshold the kernel will trigger the Conserve mode. Although the second mechanism was added to augment the first mechanism, the two triggers actually measure different things. So the second trigger actually runs regardless of whether there is AV scanning enabled.

Entering and exiting conserve mode

A FortiGate unit will enter conserve mode because it is nearly out of physical memory, or because the AV proxy has reached the maximum number of sessions it can service. The memory threshold that triggers conserve mode varies by model, but it is about 20% free memory. When memory usage rises to the point where less than 20% of the physical memory is free, the FortiGate unit enters conserve mode. A noticeable change to what is happening to traffic only occurs if the AV proxy is being used and what change happens will depend on the `av-failopen` setting.

For example, if the default `av-failopen` setting, 'pass' is being used then any files that are not in the process of being scanned will go into AV bypass mode and all new connections will automatically go into AV bypass until member availability increases to the proper threshold. Conserve mode does not normally result in sessions being flushed from the session table unless the `av-failopen` setting is 'idledrop', in which case the AV proxy will delete what it considers to be the idle connections which in turn will result in sessions being deleted in the kernel.

The FortiGate unit will leave conserve mode only when the available physical memory exceeds about 30%. When exiting conserve mode, all new sessions configured to be scanned with features requiring the AV proxy will be scanned as normal, with the exception of a unit configured with the one-shot option.

The kernel conserve mode detection runs even when no policy in any VDOM has any form of AV/DLP scanning enabled. This means that even if there is no AV scanning occurring and the memory gets low conserve mode may be triggered and informational log messages are generated to this effect, but because no AV scanning is occurring, the actions associated with Conserve mode will not actually take place.

Conserve mode effects

What happens when the FortiGate unit enters conserve mode depends on how you have `av-failopen` configured. There are four options:

off

The off setting forces the FortiGate unit to stop all traffic that is configured for content inspection by Security Profiles features that use the AV proxy. New sessions are not allowed but current sessions continue to be processed normally unless they request more memory. Sessions requesting more memory are terminated.

For example, if a security policy is configured to use antivirus scanning, the traffic it permits is blocked while in conserve mode. A policy with IPS scanning enabled continues as normal. A policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the AV proxy.

Use the off setting when security is more important than a loss of access while the problem is rectified.

pass

The pass setting allows traffic to bypass the AV proxy and continue to its destination. Since the traffic is bypassing the proxy, no Security Profiles scanning that requires the AV proxy is performed. Security Profiles scanning that does not require the AV proxy continues normally.

Use the pass setting when access is more important than security while the problem is rectified.

Pass is the default setting.

one-shot

The one-shot setting is similar to pass in that traffic is allowed when conserve mode is active. The difference is that a system configured for one-shot will force new sessions to bypass the AV proxy even after it leaves conserve mode. The FortiGate unit resumes use of the AV proxy only when the `av-failopen` setting is changed or the unit is restarted.

idledrop

The idledrop setting will recover memory and session space by terminating all the sessions associated with the host that has the most sessions open. The FortiGate may force this session termination a number of times, until enough memory is available to allow it to leave conserve mode.

The idledrop setting is primarily designed for situations in which malware may continue to open sessions until the AV proxy cannot accept more new sessions, triggering conserve mode. If your FortiGate unit is operating near capacity, this setting could cause the termination of valid sessions. Use this option with caution.

Configuring the av-failopen command

You can configure the av-failopen command using the CLI.

```
config system global
set av-failopen {off | pass | one-shot | idledrop}
end
```

The default setting is pass.

Conserve mode and session removal

It is a common misconception that one of the things that Conserve mode does is remove sessions to assist with memory, but there is no direct relationship between Conserve mode and session removal.

- The function of Conserve mode memory tracking is avoid using any more memory for scanning files in case the becomes unresponsive.
- The Session removal function is used as a last resort when the kernel becomes incapable of allocating a page of memory.

There is a mechanism to delete kernel sessions based on lack of memory. If the kernel attempts to allocate a page for any reason and a page cannot be allocated, then the session table is scanned and the oldest session in every bucket is deleted. The count of how many sessions have been deleted due to this process is visible in the 'memory_tension' count.

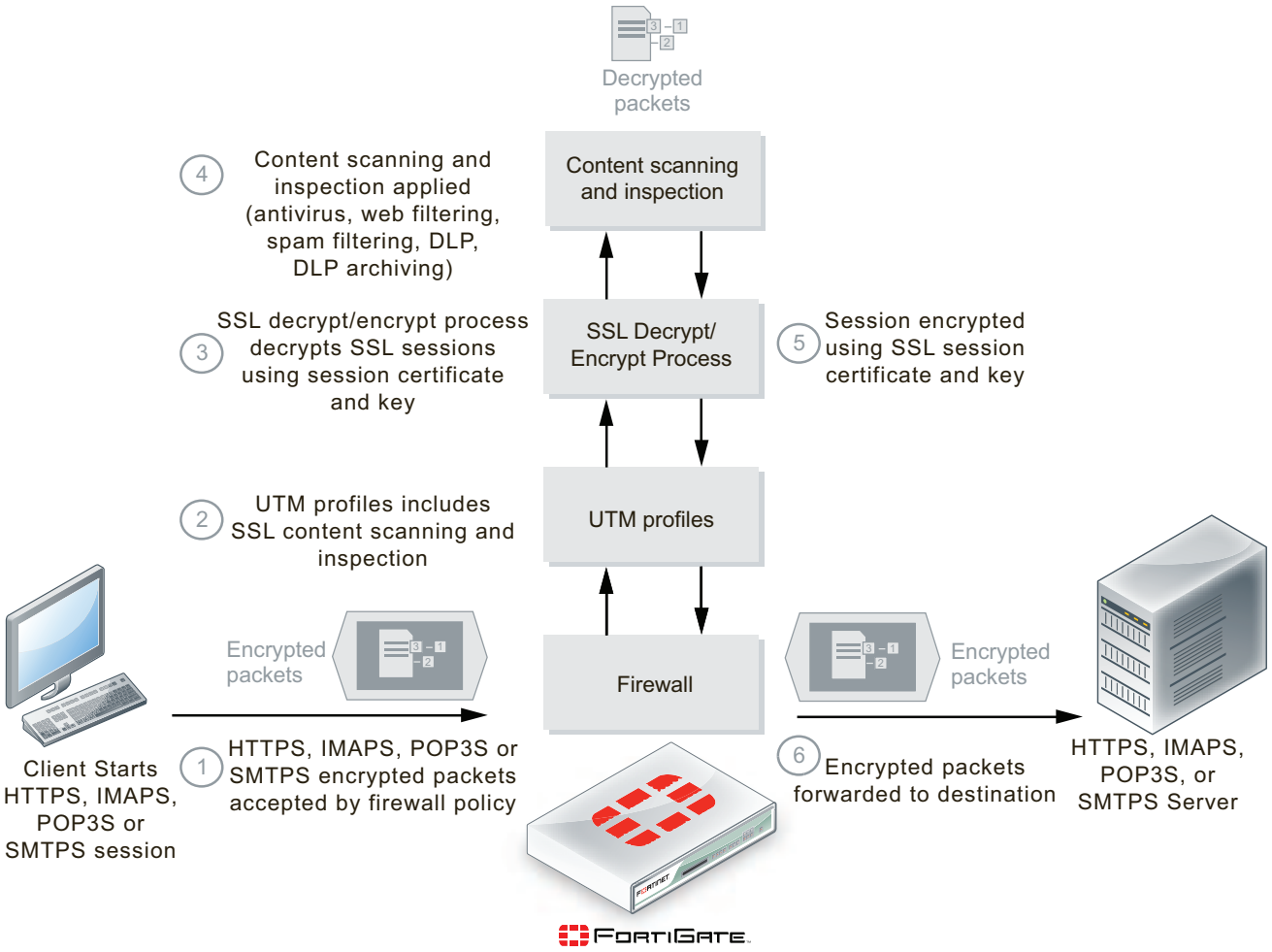
The connection between Conserve mode and session removal is that by definition page allocation cannot fail unless the device has already hit conserve mode.

SSL content scanning and inspection

If your FortiGate model supports SSL content scanning and inspection, you can apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. You can also apply DLP and DLP archiving to HTTPS, IMAPS, POP3S, and SMTPS traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:

- intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
- applies content inspection to decrypted content, including:
- HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
- HTTPS web filtering and FortiGuard web filtering
- IMAPS, POP3S, and SMTPS email filtering
- encrypts the sessions and forwards them to their destinations.

FortiGate SSL content scanning and inspection packet flow



HTTP Strict Transport Security (HSTS) Protocol

HSTS is a protocol used by Google and other web browsers to prevent man-in-the-middle attacks.

When performing deep inspection, the FortiGate intercepts the https traffic and would send its own self-signed CA certificate to the browser. If the browser is configured to use HSTS connections, it would refuse the FortiGate CA certificate since it is not on the trusted list for Google servers.

To keep the CA certificate from being refused, the HSTS settings should be cleared from the browser. Instructions for this vary between browsers.

Setting up certificates to avoid client warnings

To use SSL content scanning and inspection, you need to set up and use a certificate that supports it. FortiGate SSL content scanning and inspection intercepts the SSL keys that are passed between clients and servers during SSL session handshakes and then substitutes spoofed keys. Two encrypted SSL sessions are set up, one between the client and the FortiGate unit, and a second one between the FortiGate unit and the server. Inside the FortiGate unit the packets are decrypted.

While the SSL sessions are being set up, the client and server communicate in clear text to exchange SSL session keys. The session keys are based on the client and server certificates. The FortiGate SSL decrypt/encrypt process intercepts these keys and uses a built-in signing CA certificate named Fortinet_CA_SSLProxy to create keys to send to the client and the server. This signing CA certificate is used only by the SSL decrypt/encrypt process. The SSL decrypt/encrypt process then sets up encrypted SSL sessions with the client and server and uses these keys to decrypt the SSL traffic to apply content scanning and inspection.

Some client programs (for example, web browsers) can detect this key replacement and will display a security warning message. The traffic is still encrypted and secure, but the security warning indicates that a key substitution has occurred.

You can stop these security warnings by importing the signing CA certificate used by the server into the FortiGate unit SSL content scanning and inspection configuration. Then the FortiGate unit creates keys that appear to come from the server and not the FortiGate unit.

You can add one signing CA certificate for SSL content scanning and inspection. The CA certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported for SSL content scanning and encryption.

You can replace the default signing CA certificate, Fortinet_CA_SSLProxy, with another signing CA certificate. To do this, you need the signing CA certificate file, the CA certificate key file, and the CA certificate password.

To add a signing CA certificate for SSL content scanning and inspection

1. Obtain a copy of the signing CA certificate file, the CA certificate key file, and the password for the CA certificate.
2. Go to **System > Certificates > Local Certificates** and select **Import**.
3. Set **Type** to **Certificate**.
4. For **Certificate file,** use the **Browse** button to select the signing CA certificate file.
5. For **Key file,** use the **Browse** button to select the CA certificate key file.
6. Enter the CA certificate **Password**.
7. Select **OK**.
   The CA certificate is added to the **Local Certificates** list. In this example the signing CA certificate name is Example_CA. This name comes from the certificate file and key file name. If you want the certificate to have a different name, change these file names.
8. Add the imported signing CA certificate to the SSL content scanning and inspection configuration. Use the following CLI command if the certificate name is Example_CA.

```
config firewall ssl setting
   set caname Example_CA
end
```

The Example_CA signing CA certificate will now be used by SSL content scanning and inspection for establishing encrypted SSL sessions.

Exceptions

Periodically, you will come across situations were SSL and certificates will interfer with the smooth operation of an application or website. For instance, there is a popular application called Dropbox that does not work when deep SSL inspection is enabled. The reason for this is that the trusted certificate authority that is recognised by Dropbox is imbedded in the software and Dropbox cannot be reconfigured to recognise the FortiGate certificates that are used when deep SSL inspection is implimented.

One way to by-pass the deep inspection for Dropbox is to add dropbox.com to a local category in webfiltering and add that local category to the `ftgd-wf-ssl-exempt` list in the webfilter profile. This way any connections with dropbox.com will be exempt from deep SSL inspection.

Whenever an exception is found, the reason that it causes an issue will have to be determined in order to figure out a way to accommodate that application or website.

Configuring packet logging options

You can use a number of CLI commands to further configure packet logging.

Limiting memory use

When logging to memory, you can define the maximum amount of memory used to store logged packets.

```
config ips settings
   set packet-log-memory 256
end
```

The acceptable range is from 64 to 8192 kilobytes. This command affects only logging to memory.

Limiting disk use

When logging to the FortiGate unit internal hard disk, you can define the maximum amount of space used to store logged packets.

```
config ips settings
   set ips-packet-quota 256
end
```

The acceptable range is from 0 to 4294967295 megabytes. This command affects only logging to disk.

Configuring how many packets are captured

Since the packet containing the signature is sometimes not sufficient to troubleshoot a problem, you can specify how many packets are captured before and after the packet containing the IPS signature match.

```
config ips settings
   packet-log-history
   packet-log-post-attack
end
```

The `packet-log-history` command specifies how many packets are captured before and including the one in which the IPS signature is detected. If the value is more than `1`, the packet containing the signature is saved in

the packet log, as well as those preceding it, with the total number of logged packets equalling the `packet-log-history` setting. For example, if `packet-log-history` is set to `7`, the FortiGate unit will save the packet containing the IPS signature match and the six before it.

The acceptable range for `packet-log-history` is from 1 to 255. The default is 1.

Setting `packet-log-history` to a value larger than `1` can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

The `packet-log-post-attack` command specifies how many packets are logged after the one in which the IPS signature is detected. For example, if `packet-log-post-attack` is set to `10`, the FortiGate unit will save the ten packets following the one containing the IPS signature match.

The acceptable range for `packet-log-post-attack` is from 0 to 255. The default is 0.

Using wildcards and Perl regular expressions

Many Security Profiles feature list entries can include wildcards or Perl regular expressions.

For more information about using Perl regular expressions, see http://perldoc.perl.org/perlretut.html.

Regular expression vs. wildcard match pattern

A wildcard character is a special character that represents one or more other characters. The most commonly used wildcard characters are the asterisk (*), which typically represents zero or more characters in a string of characters, and the question mark (?), which typically represents any one character.

In Perl regular expressions, the '.' character refers to any single character. It is similar to the '?' character in wildcard match pattern. As a result:

- example.com not only matches example.com but also examplea.com, exampleb.com, examplec.com, and so on.

To add a question mark (`?`) character to a regular expression from the FortiGate CLI, enter Ctrl+V followed by ?. To add a single backslash character (`\`) to a regular expression from the CLI you must add precede it with another backslash character. For example, `example\\.com`.

To match a special character such as '.' and '*' use the escape character '\'. For example:

- To match example.com, the regular expression should be: example\.com

In Perl regular expressions, '*' means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- exam*.com matches exammmm.com but does not match example.com

To match any character 0 or more times, use '.*' where '.' means any character and the '*' means 0 or more times. For example, the wildcard match pattern exam*.com should therefore be exam.*\.com.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression "test" not only matches the word "test" but also any word that contains "test" such as "atest", "mytest",

“testimony”, “atestb”. The notation “\b” specifies the word boundary. To match exactly the word “test”, the expression should be \btest\b.

Case sensitivity

Regular expression pattern matching is case sensitive in the web and Email Filter filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of “bad language”, regardless of case.

Perl regular expression formats

The following table lists and describes some example Perl regular expressions.

Perl regular expression formats

Expression	Matches
abc	“abc” (the exact character sequence, but anywhere in the string)
^abc	“abc” at the beginning of the string
abc$	“abc” at the end of the string
a|b	Either “a” or “b”
^abc|abc$	The string “abc” at the beginning or at the end of the string
ab{2,4}c	“a” followed by two, three or four “b”s followed by a “c”
ab{2,}c	“a” followed by at least two “b”s followed by a “c”
ab*c	“a” followed by any number (zero or more) of “b”s followed by a “c”
ab+c	“a” followed by one or more b's followed by a c
ab?c	“a” followed by an optional “b” followed by a” c”; that is, either “abc” or ”ac”
a.c	“a” followed by any single character (not newline) followed by a” c “
a\.c	“a.c” exactly
[abc]	Any one of “a”, “b” and “c”
[Aa]bc	Either of “Abc” and “abc”
[abc]+	Any (nonempty) string of “a”s, “b”s and “c”s (such as “a”, “abba”, ”acbabcacaa”)
[^abc]+	Any (nonempty) string which does not contain any of “a”, “b”, and “c” (such as “defg”)
\d\d	Any two decimal digits, such as 42; same as \d{2}
/i	Makes the pattern case insensitive. For example, `/bad language/i` blocks any instance of `bad language` regardless of case.
\w+	A “word”: A nonempty sequence of alphanumeric characters and low lines (under-scores), such as foo and 12bar8 and foo_1
100\s*mk	The strings “100” and “mk” optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	“abc” when followed by a word boundary (for example, in “abc!” but not in “abcd”)
perl\B	“perl” when not followed by a word boundary (for example, in “perlert” but not in “perl stuff”)

Expression	Matches
\x	Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into (slightly) more readable parts.
/x	Used to add regular expressions within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/'. The pattern between '/' will be taken as a regular expressions, and anything after the second '/' will be parsed as a list of regular expression options ('i', 'x', etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Examples of regular expressions

Block any word in a phrase

```
/block|any|word/
```

Block purposely misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*o.*$/i
/cr[eéèêë][\+\-\*=<>\.\,;!\?%&$@\^°\$£€\{\}()\[\]\|\\_01]dit/i
```

Block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

```
/try it for free/i
/student loans/i
/you're already approved/i
/special[\+\-\*=<>\.\,;!\?%&~#$@\^°\$£€\{\}()\[\]\|\\_1]offer/i
```

Chapter 22 - SSL VPN

The following chapters are included in this document:

Introduction to SSL VPN provides useful general information about VPN and SSL, how the FortiGate unit implements them, and gives guidance on how to choose between SSL and IPsec.

Basic configuration explains how to configure the FortiGate unit and the web portal. Along with these configuration details, this chapter also explains how to grant unique access permissions, how to configure the SSL encryption key algorithm, and describes the SSL VPN OS Patch Check feature that allows a client with a specific OS patch to access SSL VPN services.

The SSL VPN client provides an overview of the FortiClient software required for tunnel mode, where to obtain the software, how to install it, and the configuration information required for remote users to connect to the internal network.

The SSL VPN web portal provides an overview of the SSL VPN web portal, with explanations of how to use and configure the web portal features.

Setup examples explores several configuration scenarios with step-by-step instructions. While the information provided is enough to set up the described SSL VPN configurations, these scenarios are not the only possible SSL VPN setups.

Introduction to SSL VPN

As organizations have grown and become more complex, secure remote access to network resources has become critical for day-to-day operations. In addition, businesses are expected to provide clients with efficient, convenient services including knowledge bases and customer portals. Employees traveling across the country or around the world require timely and comprehensive access to network resources. As a result of the growing need for providing remote/mobile clients with easy, cost-effective and secure access to a multitude of resources, the concept of a Virtual Private Network (VPN) was developed.

SSL VPNs establish connectivity using SSL, which functions at Levels 4 - 5 (Transport and Session layers). Information is encapsulated at Levels 6 - 7 (Presentation and Application layers), and SSL VPNs communicate at the highest levels in the OSI model. SSL is not strictly a Virtual Private Network (VPN) technology that allows clients to connect to remote networks in a secure way. A VPN is a secure logical network created from physically separate networks. VPNs use encryption and other security methods to ensure that only authorized users can access the network. VPNs also ensure that the data transmitted between computers cannot be intercepted by unauthorized users. When data is encoded and transmitted over the Internet, the data is said to be sent through a “VPN tunnel”. A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.

The advantages of a VPN over an actual physical private network are two-fold. Rather than utilizing expensive leased lines or other infrastructure, you use the relatively inexpensive, high-bandwidth Internet. Perhaps more important though is the universal availability of the Internet. In most areas, access to the Internet is readily obtainable without any special arrangements or long wait times.

SSL (Secure Sockets Layer) as HTTPS is supported by most web browsers for exchanging sensitive information securely between a web server and a client. SSL establishes an encrypted link, ensuring that all data passed between the web server and the browser remains private and secure. SSL protection is initiated automatically when a user (client) connects to a web server that is SSL-enabled. Once the successful connection is established, the browser encrypts all the information before it leaves the computer. When the information reaches its destination, it is decrypted using a secret (private) key. Any data sent back is first encrypted, and is decrypted when it reaches the client.

FortiOS supports the SSL and TLS versions defined below:

SSL and TLS version support table

Version	RFC
SSL 2.0	RFC 6176
SSL 3.0	RFC 6101
TLS 1.0	RFC 2246
TLS 1.1	RFC 4346
TLS 1.2	RFC 5246

SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on username, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode or tunnel mode.

Web-only mode

Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java runtime environment.

Support for SSL VPN web-only mode is built into FortiOS. The feature comprises of an SSL daemon running on the FortiGate unit, and a web portal, which provides users with access to network services and resources including HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.

In web-only mode, the FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page and the user can access the server applications behind the FortiGate unit.

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

FortiGate SSL VPN web portals have a 1- or 2-column page layout and portal functionality is provided through small applets called widgets. Widget windows can be moved or minimized. The controls within each widget depend on its function. There are predefined web portals and the administrator can create additional portals.

Configuring the FortiGate unit involves selecting the appropriate web portal configuration in the user group settings. These configuration settings determine which server applications can be accessed. SSL encryption is used to ensure traffic confidentiality.

The following table lists the operating systems and web browsers supported by SSL VPN web-only mode.

VPN Web-only Mode, supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 32-bit SP1	• Microsoft Internet Explorer versions 9, 10 and 11 • Mozilla Firefox version 33
Microsoft Windows 7 64-bit SP1	• Microsoft Internet Explorer versions 9, 10 and 11 • Mozilla Firefox version 33
Linux CentOS version 5.6 and Ubuntu version 12.0.4	• Mozilla Firefox version 5.6

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Tunnel mode

Tunnel mode offers remote users the freedom to connect to the internal network using the traditional means of web-based access from laptop computers, as well as from airport kiosks, hotel business centers, and Internet cafés. If the applications on the client computers used by your user community vary greatly, you can deploy a dedicated SSL VPN client to any remote client through its web browser. The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the web browser and the FortiGate unit. Another option is split tunneling, which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This conserves bandwidth and alleviates bottlenecks.

In tunnel mode, remote clients connect to the FortiGate unit and the web portal login page using Microsoft Internet Explorer, Firefox, Mac OS, or Linux. The FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page dictated by the user group authentication settings. If the user does not have the SSL VPN client installed, they will be prompted to download the SSL VPN client (an ActiveX or Java plugin) and install it using controls provided through the web portal. SSL VPN tunnel mode can also be initiated from a standalone application on Windows, Mac OS X, and Linux (see below).

Remote clients in tunnel mode cannot connect to the web portal using Chrome as it is not supported. Refer to the Release Notes for more information.

SSL VPN Tunnel client standalone installer (build 2300) supported operating systems

Operating System	Release
Microsoft Windows	• 8.1 (32-bit & 64-bit), 8 (32-bit & 64-bit), 7 (32-bit & 64-bit), and XP SP3 in .exe and .msi formats
Linux	• CentOS and Ubuntu in .tar.gz format
Virtual Desktop	• In .jar format for Microsoft Windows 7 SP1 (32-bit)

When the user initiates a VPN connection with the FortiGate unit through the SSL VPN client, the FortiGate unit establishes a tunnel with the client and assigns the client a virtual IP address from a range of reserved addresses. The client uses the assigned IP address as its source address for the duration of the connection. After the tunnel has been established, the user can access the network behind the FortiGate unit.

Configuring the FortiGate unit to establish a tunnel with remote clients involves enabling the feature through SSL VPN configuration settings and selecting the appropriate web portal configuration for tunnel-mode access in the user group settings. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

The user account used to install the SSL VPN client on the remote computer must have administrator privileges.

If you are using Windows Vista, you must disable UAC (User Account Control) before installing the SSL VPN tunnel client. IE7 in Windows Vista runs in Protected Mode by default. To install SSL VPN client ActiveX, you need to launch IE7 by using 'Run as administrator' (right-click the IE7 icon and select 'Run as administrator').

For information about client operating system requirements, see the Release Notes for your FortiGate firmware. For information on configuring tunnel mode, see Basic configuration on page 2155.

Port forwarding mode

While tunnel mode provides a Layer 3 tunnel that users can run any application over, the user needs to install the tunnel client, and have the required administrative rights to do so. In some situations, this may not be desirable, yet the simple web mode does not provide enough flexibility for application support (for example, if you wish to use an email client that communicates with a POP3 server). The port forward mode, or proxy mode, provides this middle ground between web mode and tunnel mode.

SSL VPN port forwarding listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the FortiGate unit, which then forwards the traffic to the application server.

The port forward module is implemented with a Java applet, which is downloaded and runs on the user's computer. The applet provides the up-to-date status information such as addressing and bytes sent and received.

On the user end, the user logs into the FortiGate SSL VPN portal, and selects a port forward bookmark configured for a specific application. The bookmark defines the server address and port as well as which port to listen to on the user's computer.

The user must configure the application on the PC to point to the local proxy instead of the application server. For information on this configuration change, see the application documentation.

This mode only supports client/server applications that are using a static TCP port. It will not support client/server applications using dynamic ports or traffic over UDP.

For information on configuring a port forward tunnel, see Basic configuration on page 2155.

Application support

With Citrix application servers, the server downloads an ICA configuration file to the user's PC. The client application uses this information to connect to the Citrix server. The FortiGate unit will read this file and append a SOCKS entry to set the SOCKS proxy to 'localhost'. The Citrix client will then be able to connect to the SSL VPN port forward module to provide the connection. When configuring the port forwarding module, a selection is available for Citrix servers.

For Windows Remote Desktop Connections, when selecting the RDP option, the tunnel will launch the RDP client and connect to the local loopback address after the port forward module has been initiated.

RDP Native, in some instances, may not be supported. If this is the case, use Internet Explorer and disable ActiveX Filtering.

Antivirus and firewall host compatibility

The following tables list the antivirus and firewall client software packages that are supported in FortiOS.

Supported Windows XP antivirus and firewall software

Product supported	Antivirus	Firewall
Symantec Endpoint Protection V11	•	•
Kaspersky Antivirus 2009	•	
McAfee Security Center v8.1	•	•
Trend Micro Internet Security Pro	•	•
F-Secure Internet Security 2009	•	•

Supported Windows 7 32-bit and 64-bit antivirus and firewall software

Product supported	Antivirus	Firewall
CA Internet Security 2011	•	•
AVG Internet Security 2011		
F-Secure Internet Security 2011	•	•
Kaspersky Internet Security 2011	•	•
McAfee Internet Security 2011	•	•
Norton 360TM Version 4.0	•	•
NortonTM Internet Security 2011	•	•
Panda Internet Security 2011	•	•
Sophos Security Suite	•	•
Trend Micro Titanium Internet Security	•	•
ZoneAlarm Security Suite	•	•
Symantec Endpoint Protection Small Business Edition 12.0	•	•

Traveling and security

Because SSL VPN provides a means for “on-the-go” users to dial in to the network while away from the office, you need to ensure that wherever and however they choose to dial in is secure, and not potentially compromising the

corporate network.

When setting up the portal, you can include two options to ensure corporate data is safe; a host check for antivirus software, and a cache cleaner.

Host check

You can enable a host integrity checker to scan the remote client. The integrity checker probes the remote client computer to verify that it is safe before access is granted. Security attributes recorded on the client computer (for example, in the Windows registry, in specific files, or held in memory due to running processes) are examined and uploaded to the FortiGate unit. For more information, see Basic configuration on page 2155.

Host Check is applicable for both SSLVPN Web Mode and SSLVPN Tunnel mode.

Cache cleaning

You can enable a cache cleaner to remove any sensitive data that would otherwise remain on the remote computer after the session ends. For example, all cache entries, browser history, cookies, encrypted information related to user authentication, and any temporary data generated during the session are removed from the remote computer. If the client's browser cannot install and run the cache cleaner, the user is not allowed to access the SSL-VPN portal. For more information, see Basic configuration on page 2155.

SSL VPN and IPv6

FortiOS supports SSL VPN with IPv6 addressing, and is available for all the java applets (Telnet, VNC, RDP, and so on). IPv6 configurations for security policies and addressing include:

- Policy matching for IPv6 addresses
- Support for DNS resolving in SSL VPN
- Support IPv6 for ping
- FTP applications
- SMB

In essentially any of the following instructions, replace **IPv4** with **IPv6** to achieve the same desired results, but for IPv6 addresses and configurations.

Basic configuration

Configuring SSL VPN involves a number of configurations within FortiOS that you need to complete to make it all come together. This chapter describes the components required, and how and where to configure them to set up the FortiGate unit as an SSL VPN server. The configurations and steps are high level, to show you the procedures needed, and where to locate the options in FortiOS. For real-world examples, see Setup examples on page 2200.

There are three or four key steps to configuring an SSL VPN tunnel. The first three in the points below are mandatory, while the others are optional. This chapter outlines these key steps as well as additional configurations for tighter security and monitoring.

The key steps are:

- Create user accounts and user groups for the remote clients.
  (User accounts and groups on page 2155)
- Create a web portal to define user access to network resources.
  (Configuring SSL VPN web portals on page 2160)
- Configure the security policies.
  (Configuring security policies on page 2167)
- For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.
  (Routing in tunnel mode on page 2173)
- Setup logging of SSL VPN activities.
  (SSL VPN logs on page 2180)

This section contains the following information:

User accounts and groups
Configuring SSL VPN web portals
Configuring security policies
Configuring encryption key algorithms
Additional configuration options

User accounts and groups

The first step for an SSL VPN tunnel is to add the users and user groups that will access the tunnel. You may already have users defined for other authentication-based security policies.

The user group is associated with the web portal that the user sees after logging in. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

To create a user account:

- In the web-based manager, go to **User & Device > User > User Definition**, and select **Create New.**
- In the CLI, use the commands in `config user local`.

All users accessing the SSL tunnel must be in a firewall user group. User names can be up to 64 characters long.

To create user groups:

- In the web-based manager, go to **User & Device > User > User Groups** and select **Create New**.
- In the CLI, use the commands in `config user group`.

Authentication

Remote users must be authenticated before they can request services and/or access network resources through the web portal. The authentication process can use a password defined on the FortiGate unit or optionally use established external authentication mechanisms such as RADIUS or LDAP.

To authenticate users, you can use a plain text password on the local FortiGate unit, forward authentication requests to an external RADIUS, LDAP or TACACS+ server, or utilize PKI certificates.

For information about how to create RADIUS, LDAP, TACACS+ or PKI user accounts and certificates, see the Authentication Guide.

FortiOS supports LDAP password renewal notification and updates through SSL VPN. Configuration is enabled using the CLI commands:

```
config user ldap
   edit <username>
       set server <domain>
       set password-expiry-warning enable
       set password-renewal enable
end
```

For more information, see the Authentication Guide.

MAC host check

When a remote client attempts to log in to the portal, you can have the FortiGate unit check against the client's MAC address to ensure that only a specific computer or device is connecting to the tunnel. This can ensure better security should a password be compromised.

MAC addresses can be tied to specific portals and can be either the entire MAC address or a subset of the address. MAC host checking is configured in the CLI using the folowing commands:

```
conf vpn ssl web portal
   edit portal
      set mac-addr-check enable
      set mac-addr-action allow
         config mac-addr-check-rule
            edit "rule1"
               set mac-addr-list 01:01:01:01:01:01 08:00:27:d4:06:5d
               set mac-addr-mask 48
         end
   end
```

IP addresses for users

After the FortiGate unit authenticates a request for a tunnel-mode connection, the FortiGate unit assigns the SSL VPN client an IP address for the session. The address is assigned from an IP Pool, which is a firewall address

defining an IP address range.

Take care to prevent overlapping IP addresses. Do not assign to clients any IP addresses that are already in use on the private network. As a precaution, consider assigning IP addresses from a network that is not commonly used (for example, 10.254.254.0/24).

To set tunnel-mode client IP address range - web-based manager:

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Enter a **Name**, for example, `SSL_VPN_tunnel_range`.
3. Select a **Type** of **IP Range**.
4. In the **Subnet/IP Range** field, enter the starting and ending IP addresses that you want to assign to SSL VPN clients, for example `10.254.254.[80-100]`.
5. In **Interface**, select **Any**.
6. Select **OK**.

To set tunnel-mode client IP address range - CLI:

If your SSL VPN tunnel range is for example 10.254.254.80 - 10.254.254.100, you could enter

```
config firewall address
   edit SSL_tunnel_users
      set type iprange
      set end-ip 10.254.254.100
      set start-ip 10.254.254.80
   end
```

DHCP relay of IP address

The FortiGate can get an IP address via DHCP server for SSL VPN services, however it is only configurable in the CLI Console by editing the ssl.root interface.

To enable DHCP relay service and relay IP address - CLI:

```
config system interface
   edit ssl.root
      set dhcp-relay-service [enable|disable]
      set dhcp-relay-ip
   next
end
```

Authentication of remote users

When remote users connect to the SSL VPN tunnel, they must perform authentication before being able to use the internal network resources. This can be as simple as assigning users with their own passwords, connecting to an LDAP server or using more secure options. FortiOS provides a number of options for authentication as well as security option for those connected users.

The web portal can include bookmarks to connect to internal network resources. A web (HTTP/HTTPS) bookmark can include login credentials so that the FortiGate unit automatically logs the user into the website. This means that the user logs into the SSL VPN and then does not have to enter any more credentials to visit preconfigured web sites.

Both the administrator and the end user can configure bookmarks, including SSO bookmarks. To add bookmarks as a web portal user, see The SSL VPN web portal on page 2184.

Setting the client authentication timeout

The client authentication timeout controls how long an authenticated user will remain connected. When this time expires, the system forces the remote client to authenticate again. As with the idle timeout, a shorter period of time is more secure. The default value is 28800 seconds (8 hours). You can only modify this timeout value in the CLI.

For example, to change the authentication timeout to 18 000 seconds, enter the following commands in the CLI:

```
config vpn ssl settings
   set auth-timeout 18000
end
```

You can also set the idle timeout for the client, to define how long the user does not access the remote resources before they are logged out. For information see User accounts and groups on page 2155.

Allow one-time login per user

You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again.

To allow one-time login per user - web-based manager:

Go to **VPN > SSL > Portals**, select a portal, and enable **Limit Users to One SSL-VPN Connection at a Time.** It is disabled by default.

To allow one-time login per user - CLI:

```
config vpn ssl web portal
   edit <portal_name>
      set limit-user-logins enable
end
```

Strong authentication with security certificates

The FortiGate unit supports strong (two-factor) authentication through X.509 security certificates (version 1 or 3). The FortiGate unit can require clients to authenticate using a certificate, and the client can require the FortiGate unit to authenticate using a certificate.

For information about obtaining and installing certificates, see the Authentication Guide.

You can select the **Require Client Certificate** option so that clients must authenticate using certificates. The client browser must have a local certificate installed, and the FortiGate unit must have the corresponding CA certificate installed.

When the remote client initiates a connection, the FortiGate unit prompts the client browser for its client-side certificate as part of the authentication process.

To require client authentication by security certificates - web-based manager:

1. Go to **VPN > SSL > Settings**.
2. Select **Require Client Certificate**.
3. Select **Apply**.

To require client authentication by security certificates - CLI:

```
config vpn ssl settings
   set reqclientcert enable
end
```

If your SSL VPN clients require strong authentication, the FortiGate unit must offer a CA certificate that the client browser has installed.

In the FortiGate unit SSL VPN settings, you can select which certificate the FortiGate offers to authenticate itself. By default, the FortiGate unit offers its factory installed (Fortinet_CA_SSLProxy) certificate from Fortinet to remote clients when they connect. If you leave the default setting, a warning appears that recommends you purchase a certificate for your domain and upload it for use.

To enable FortiGate unit authentication by certificate - web-based manager:

1. Go to **VPN > SSL > Settings**.
2. From the **Server Certificate** list, select the certificate that the FortiGate unit uses to identify itself to SSL VPN clients.
3. Select **Apply**.

To enable FortiGate unit authentication by certificate - CLI:

For example, to use the `example_cert` certificate

```
config vpn ssl settings
   set servercert example_cert
end
```

FortiOS will check the server certificate to verify that the certificate is valid. Only valid server certificates should be used.

NSA Suite B cryptography support

FortiOS supports the use of ECDSA Local Certificates for SSL VPN Suite B. The National Security Agency (NSA) developed Suite B algorithms in 2005 to serve as a cryptographic base for both classified and unclassified information at an interoperable level.

FortiOS allows you to import, generate, and use ECDSA certificates defined by the Suite B cryptography set. To generate ECDSA certificates, use the following command in the CLI:

```
exec vpn certificate local generate ec <certificate-name_str> <elliptic-curve-name>
    <subject_str> [<optional_information>]
```

Configuring SSL VPN web portals

The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

FortiOS supports LDAP password renewal notification and updates through SSL VPN. Configuration is enabled using the CLI commands:

```
config user ldap
   edit <username>
       set server <domain>
       set password-expiry-warning enable
       set password-renewal enable
end
```

For more information, see the Authentication Guide.

This step in the configuration of the SSL VPN tunnel sets up the infrastructure; the addressing, encryption, and certificates needed to make the initial connection to the FortiGate unit. This step is also where you configure what the remote user sees with a successful connection. The portal view defines the resources available to the remote users and the functionality they have on the network.

SSL connection configuration

To configure the basic SSL VPN settings for encryption and login options, go to **VPN > SSL > Settings.**

Listen on Interface(s)	Define the interface which the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.
Restrict Access	Restrict accessibility to either **Allow access from any host** or to **Limit access to specific hosts** as desired. If selecting the latter, you must specify the hosts.
Server Certificate	Select the signed server certificate to use for authentication. If you leave the default setting (Fortinet_CA_SSLProxy), the FortiGate unit offers its built-in certificate from Fortinet to remote clients when they connect. A warning appears that recommends you purchase a certificate for your domain and upload it for use.
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the Authentication Guide.
Idle Logout	Type the period of time (in seconds) that the connection can remain inactive before the user must log in again. The range is from 10 to 28800 seconds. Setting the value to 0 will disable the idle connection timeout. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.
Address Range	Select **Specify custom IP ranges** to select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients.
DNS Server	Enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
Specify WINS Servers	Enable to access options for entering up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
Allow Endpoint Registration	Select so that FortiClient registers with the FortiGate unit when connecting. If you configured a registration key by going to **System > Config > Advanced**, the remote user is prompted to enter the key. This only occurs on the first connection to the FortiGate unit.

Portal configuration

The portal configuration determines what the remote user sees when they log in to the portal. Both the system administrator and the user have the ability to customize the SSL VPN portal.

To view the portals settings page, go to **VPN > SSL > Portals**.

There are three pre-defined default portal configurations available:

- *full-access*
- *tunnel-access*
- *web-access*

Each portal type includes similar configuration options. Select between the different portals by double-clicking one of the default portals in the list. You can also create a custom portal by selecting the **Create New** option at the top.

Name	The name for the portal.
Enable Tunnel Mode	If your web portal provides tunnel mode access, you need to configure the **Tunnel Mode** widget. These settings determine how tunnel mode clients are assigned IPv4 addresses.
Enable Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route. If you enable split tunneling, you are required to set the **Routing Address**, which is the address that your corporate network is using. Traffic intended for the Routing Address will not be split from the tunnel.
Source IP Pools	Select an IPv4 Pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Enable IPv6 Tunnel Mode	If your web portal provides tunnel mode access, you need to configure the **Tunnel Mode** widget. These settings determine how tunnel mode clients are assigned IPv6 addresses.
Enable IPv6 Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route. This applies only to IPv6 tunnels. If you enable split tunneling, you are required to set the **Routing Address**, which is the address that your corporate network is using. Traffic intended for the Routing Address will not be split from the tunnel.
Source IPv6 Pools	Select an IPv6 Pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. **Save Password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. **Auto Connect** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. **Always Up (Keep Alive)** - When enabled, if the user selects this option, the FortiClient should try to reconnect once it detects the VPN connection is down unexpectedly (not manually disconnected by user).

Enable Web Mode	Select to enable web mode access.
Portal Message	This is a text header that appears on the top of the web portal.
Theme	A color styling specifically for the web portal.
Page Layout	Select one column or two column layouts for the widgets that appear on the web portal page.
Include Status Information	Select to display the **Status Information** widget on the portal page. The **Status Information** widget displays the login name of the user, the amount of time the user has been logged in, and the inbound and out-bound traffic statistics.
Include Connection Tool	Select to display the Connection Tool widget on the portal page. Use the **Connection Tool** widget to connect to a internal network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.
Include FortiClient Down-load	Select to include the **FortiClient Download** option in the web portal. This is enabled by default.
Prompt Mobile Users to Download FortiClient Application	If a remote user is using a web browser to connects to the SSL VPN in web mode, they are prompted to download the FortiClient application. The remote user can accept or reject the notification. If the user accepts, they are redirected to the FortiClient web site.
Include Login History	Select to include user login history on the web portal.
Enable User Bookmarks	Select to include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window appears with the web page. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
Limite Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same cre-dentials again. This option is disabled by default.

If your network configuration does not contain a default SSL VPN portal, you might receive the error message “Input value is invalid” when you attempt to access **VPN > SSL > Portals**.

To enable a default portal - CLI:

```
config vpn ssl settings
   set default-portal <full-access | tunnel-access |
    web-access>
end
```

Adding bookmarks

A web bookmark can include login credentials to automatically log the SSL VPN user into the website. When the administrator configures bookmarks, the website credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the website.

To add a bookmark - web-based manager:

1. On the **VPN > SSL > Portals** page, ensure **Enable User Bookmarks** is enabled.
2. Select **Create New** and enter the following information:

Category	Select a category, or group, to include the bookmark. If this is the first bookmark added, you will be prompted to add a category. Otherwise, select **Create** from the drop-down list.
Name	Enter a name for the bookmark.
Type	Select the type of link from the drop-down list. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
URL	Enter the IP address source.
Description	Enter a brief description of the link.
Single Sign-On	Enable if you wish to use Single Sign-On (SSO) for any links that require authentication. When including a link using SSO, be sure to use the entire URL. For example, http://10.10.1.0/login, rather than just the IP address.

3. Select **OK**.

For more configuration options, see Configuring SSL VPN web portals on page 2160.

Personal bookmarks

The administrator has be ability to view bookmarks the remote client has added to their SSL VPN login in the bookmarks widget. This enables the administrator to monitor and, if needed, remove unwanted bookmarks that do not meet with corporate policy.

To view and maintain remote client bookmarks, go to **VPN > SSL > Personal Bookmarks**.

For more information about available bookmark applications, see Applications available in the web portal on page 2192

SSL VPN Realms

You can go to **VPN > SSL > Realms** and create custom login pages for your SSL VPN users. You can use this feature to customize the SSL VPN login page for your users and also to create multiple SSL VPN logins for different user groups.

In order to create a custom login page using the web-based manager, this feature must be enabled using **Feature Select**.

Before you begin, copy the default login page text to a separate text file for safe-keeping. Afterward, if needed, you can restore the text to the original version.

To configure SSL VPN Realms - web-based manager:

1. Configure a custom SSL VPN login by going to **VPN > SSL > Realms** and selecting **Create New**. Users access different portals depending on the URL they enter.
2. The first option in the custom login page is to enter the path of the custom URL.
   This path is appended to the address of the FortiGate unit interface to which SSL VPN users connect. The actual path for the custom login page appears beside the URL path field.
3. You can also limit the number of users that can access the custom login at any given time.
4. You can use HTML code to customize the appearance of the login page.
5. After adding the custom login, you must associate it with the users that will access the custom login. Do this by going to **VPN > SSL > Settings** and adding a rule to the **Authentication/Portal Mapping** section.
6. Under **Authentication/Portal Mapping**, click **Create New** and select the user group(s) and the associated Realm.

To configure SSL VPN Realms - CLI:

```
config vpn ssl web realm
   edit <url-path>
      set login-page <content_str>
      set max-concurrent-user <int>
      set virtual-host <hostname_str>
   end
```

Where the following variables are set:

Variable	Description	Default
`edit <url-path>`	Enter the URL path to access the SSL-VPN login page. Do not include “http://”.	No default.
`login-page <content_str>`	Enter replacement HTML for SSL-VPN login page.	No default.
`max-concurrent-user <int>`	Enter the maximum number of concurrent users allowed. Range 0-65 535. 0 means unlimited.	0
`virtual-host <hostname_str>`	Enter the virtual host name for this realm. Optional. Maximum length 255 characters.	No default.

Tunnel mode and split tunneling

If you want your web portal to have tunnel mode access, select **Tunnel Mode** when creating a new portal. Enable **Split Tunneling** so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user’s other traffic follows its normal route.

When you enable split tunneling, you are required to set the **Routing Address**, which is the address that your corporate network is using. Traffic intended for the Routing Address will not be split from the tunnel.

CLI Syntax:

```
config vpn ssl web portal
   edit "full-access"
      set tunnel-mode enable
      set web-mode enable
      set mac-addr-check enable
      set ip-pools "SSLVPN_TUNNEL_ADDR1"
      set split-tunneling-routing-address "Internal_subnet"
```

Port forwarding

Port forwarding provides a method of connecting to application servers without configuring a tunnel mode connection, and requiring the installation of a tunnel mode client. Set up the portal as described at Configuring SSL VPN web portals on page 2160. To configure the application, create a bookmark with the **Type** field set to **Port Forward**.

Ensure that **Port Forward** is enabled in the **Applications** list.

Configuring security policies

You will need at least one SSL VPN security policy. This is an identity-based policy that authenticates users and enables them to access the SSL VPN web portal. The SSL VPN user groups named in the policy determine who can authenticate and which web portal they will use. From the web portal, users can access protected resources or download the SSL VPN tunnel client application.

This section contains the procedures needed to configure security policies for web-only mode operation and tunnel-mode operation. These procedures assume that you have already completed the procedures outlined in Configuring security policies on page 2167.

If you will provide tunnel mode access, you will need a second security policy—an ACCEPT tunnel mode policy to permit traffic to flow between the SSL VPN tunnel and the protected networks.

Firewall addresses

Before you can create security policies, you need to define the firewall addresses you will use in those policies. For both web-only and tunnel mode operation, you need to create firewall addresses for all of the destination networks and servers to which the SSL VPN client will be able to connect.

For tunnel mode, you will already have defined firewall addresses for the IP address ranges that the FortiGate unit will assign to SSL VPN clients.

The source address for your SSL VPN security policies will be the predefined “all” address. Both the address and the netmask are `0.0.0.0`. The “all” address is used because VPN clients will be connecting from various addresses, not just one or two known networks. For improved security, if clients will be connecting from one or two known locations you should configure firewall addresses for those locations, instead of using the “all” address.

To create a firewall address, in the web-based manager, go to **Policy & Objects > Objects > Addresses**, and select **Create New.**

Create an SSL VPN security policy

At minimum, you need one SSL VPN security policy to authenticate users and provide access to the protected networks. You will need additional security policies only if you have multiple web portals that provide access to different resources. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

The SSL VPN security policy specifies:

- The incoming interface that corresponds to the ssl.root interface.
- The SSL VPN user groups that can use the security policy.
- The times (schedule) and types of services that users can access.
- The UTM features and logging that are applied to the connection.

Do not use ALL as the destination address. If you do, you will see the “Destination address of Split Tunneling policy is invalid” error when you enable Split Tunneling.

To create an SSL-VPN security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New.**
2. Enter the following information:

Incoming Interface	Select the virtual SSL VPN interface, such as **ssl.root.**
Source Address	Select **all**.
Source User(s)	Select to allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See Configuring security policies on page 2167.
Outgoing Interface	Select the FortiGate network interface that connects to the protected network.
Destination Address	Select the firewall address you created that represents the networks and servers to which the SSL VPN clients will connect. If you want to associate multiple firewall addresses or address groups with the **Destination Interface/Zone**, from **Destination Address**, select the plus symbol. In the dialog box, move the firewall addresses or address groups from the **Available Addresses** section to the **Members** section, then select **OK**.
Service	Select services in the left list and use the right arrow button to move them to the right list. Select the ALL service to allow the user group access to all services.
Action	Select **Accept**.

Your identity-based policies are listed in the security policy table. The FortiGate unit searches the table from the top down to find a policy to match the client’s user group. Using the move icon in each row, you can change the

order of the policies in the table to ensure the best policy will be matched first. You can also use the icons to edit or delete policies. Furthermore, you can drag and drop policies in the policy list to rearrange their order.

To create an SSL VPN security policy - CLI:

Create the SSL VPN security policy by entering the following CLI commands.

```
config firewall policy
   edit <id>
      set srcintf ssl.root(sslvpn tunnel interface)
      set dstintf port2
      set srcaddr all
      set dstaddr OfficeLAN
      set nat enable
   end
```

Create a tunnel mode security policy

If your SSL VPN will provide tunnel mode operation, you need to create a security policy to enable traffic to pass between the SSL VPN virtual interface and the protected networks. This is in addition to the SSL VPN security policy that you created in the preceding section.

The SSL VPN virtual interface is the FortiGate unit end of the SSL tunnel that connects to the remote client. It is named `ssl.<vdom_name>`. In the root VDOM, for example, it is named `ssl.root`. If VDOMs are not enabled on your FortiGate unit, the SSL VPN virtual interface is also named ssl.root.

To configure the tunnel mode security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface, such as **ssl.root.**
Source Address	Select the firewall address you created that represents the IP address range assigned to SSL VPN clients, such as SSL_VPN_tunnel_users.
Source User(s)	Select to allow access only to holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field. See Configuring security policies on page 2167.
Outgoing Interface	Select the FortiGate network interface that connects to the protected network.
Destination Address	Select the firewall address that represents the networks and servers to which the SSL VPN clients will connect. To select multiple firewall addresses or address groups, select the plus sign next to the drop-down list.
Service	Select services in the left list and use the right arrow button to move them to the right list. Select the ALL service to allow the user group access to all services.

Action	Select **Accept**.
Enable NAT	Select **Enable NAT. (Optional)**

To configure the tunnel mode security policy - CLI:

```
config firewall policy
   edit <id>
      set srcintf ssl.root(sslvpn tunnel interface)
      set dstintf <dst_interface_name>
      set srcaddr <tunnel_ip_address>
      set dstaddr <protected_network_address_name>
      set schedule always
      set service ALL
      set nat enable
   end
```

This policy enables the SSL VPN client to initiate communication with hosts on the protected network. If you want to enable hosts on the protected network to initiate communication with the SSL VPN client, you should create another Accept policy like the preceding one but with the source and destination settings reversed.

You must also add a static route for tunnel mode operation.

Routing for tunnel mode

If your SSL VPN operates in tunnel mode, you must add a static route so that replies from the protected network can reach the remote SSL VPN client.

To add the tunnel mode route - web-based manager:

1. Go to **Router > Static > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the **Destination IP/Mask** of the tunnel IP address that you assigned to the users of the web portal.
3. Select the SSL VPN virtual interface for the **Device**.
4. Select **OK**.

To add the tunnel mode route - CLI:

If you assigned 10.11.254.0/24 as the tunnel IP range, you would enter:

```
config router static
   edit <id>
      set device ssl.root
      set dst 10.11.254.0/24
end
```

Split tunnel Internet browsing policy

With split tunneling disabled, all of the SSL VPN client's requests are sent through the SSL VPN tunnel. But the tunnel mode security policy provides access only to the protected networks behind the FortiGate unit. Clients will receive no response if they attempt to access Internet resources. You can enable clients to connect to the Internet through the FortiGate unit using a split tunnel Internet browsing policy.

To add an Internet browsing policy:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Source Address	Select the firewall address you created that represents the IP address range assigned to SSL VPN clients.
Outgoing Interface	Select the FortiGate network interface that connects to the Internet.
Destination Address	Select **All**.
Action	Select **Accept**.
Enable NAT	Select **Enable**.

To configure the Internet browsing security policy - CLI:

To enable browsing the Internet through port1, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
      set dstintf port1
      set srcaddr SSL_tunne_users
      set dstaddr all
      set schedule always
      set service ALL
      set nat enable
end
```

Enabling a connection to an IPsec VPN

You might want to provide your SSL VPN clients access to another network, such as a branch office, that is connected by an IPsec VPN. To do this, you need only to add the appropriate security policy. For information about route-based and policy-based IPsec VPNs, see the IPsec VPN Guide.

Route-based connection

To configure interconnection with a route-based IPsec VPN - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Source Address	Select the firewall address that represents the IP address range assigned to SSL VPN clients.
Outgoing Interface	Select the virtual IPsec interface for your IPsec VPN.

Destination Address	Select the address of the IPsec VPN remote protected subnet.
Action	Select **ACCEPT**.
Enable NAT	Enable.

To configure interconnection with a route-based IPsec VPN - CLI:

If, for example, you want to enable SSL VPN users to connect to the private network (address name OfficeAnet) through the toOfficeA IPsec VPN, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
      set dstintf toOfficeA
      set srcaddr SSL_tunnel_users
      set dstaddr OfficeAnet
      set action accept
      set nat enable
      set schedule always
      set service ALL
end
```

Policy-based connection

To configure interconnection with a policy-based IPsec VPN - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information and select **OK**.

Incoming Interface	Select the virtual SSL VPN interface (**ssl.root**, for example).
Source Address	Select the firewall address that represents the IP address range assigned to SSL VPN clients.
Outgoing Interface	Select the FortiGate network interface that connects to the Internet.
Destination Address	Select the address of the IPsec VPN remote protected subnet.

3. Configure inbound NAT from the CLI:

```
config firewall policy
   edit 0
      set natinbound enable
   end
```

To configure interconnection with a policy-based IPsec VPN - CLI:

If, for example, you want to enable SSL VPN users to connect to the private network (address name OfficeAnet) through the OfficeA IPsec VPN, you would enter:

```
config firewall policy
   edit 0
      set srcintf ssl.root
      set dstintf port1
      set srcaddr SSL_tunnel_users
```

```
            set dstaddr OfficeAnet
            set action ipsec
            set schedule always
            set service ALL
            set inbound enable
            set outbound enable
            set natinbound enable
            set vpntunnel OfficeA
      end
```

In this example, port1 is connected to the Internet.

Configuring encryption key algorithms

The FortiGate unit supports a range of cryptographic cipher suites to match the capabilities of various web browsers. The web browser and the FortiGate unit negotiate a cipher suite before any information (for example, a user name and password) is transmitted over the SSL link. You can only configure encryption key algorithms for SSL VPN in the CLI.

To configure encryption key algorithms - CLI:

Use the following CLI command,

```
config vpn ssl settings
   set algorithm <cipher_suite>
end
```

where one of the following variables replaces <*cipher_suite*>:

Variable	Description
`low`	Use any cipher suite; AES, 3DES, RC4, or DES.
`medium`	Use a 128-bit or greater cipher suite; AES, 3DES, or RC4.
`high`	Use a ciper suite grather than 128 bits; AES or 3DES.

Note that the `algorithm <cipher_suite>` syntax is only available when the `sslvpn-enable` attribute is set to **enable**.

Additional configuration options

Beyond the basics of setting up the SSL VPN, you can configure a number of other options that can help to ensure your internal network is secure and can limit the possibility of attacks and viruses entering the network from an outside source.

Routing in tunnel mode

If you are creating a SSL VPN connection in tunnel mode, you need to add a static route so that replies from the protected network can reach the remote SSL VPN client.

To add the tunnel mode route - web-based manager:

1. Go to **Router > Static > Static Routes** and select **Create New**.
   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.

2. Enter the **Destination IP/Mask** of the tunnel IP address that you assigned to the users of the web portal.
3. Select the SSL VPN virtual interface for the **Device**.
4. Select **OK**.

To add the tunnel mode route - CLI:

If you assigned 10.11.254.0/24 as the tunnel IP range, you would enter:

```
config router static
   edit <id>
      set device ssl.root
      set dst 10.11.254.0/24
end
```

Changing the port number for web portal connections

You can specify a different TCP port number for users to access the web portal login page through the HTTPS link. By default, the port number is 443 and users can access the web portal login page using the following default URL:

`https://<FortiGate_IP_address>:443/remote/login`

where `<FortiGate_IP_address>` is the IP address of the FortiGate interface that accepts connections from remote users.

To change the SSL VPN port - web-based manager:

1. If **Current VDOM** appears at the bottom left of the screen, select **Global** from the list of VDOMs.
2. Go to **VPN > SSL > Settings**.
3. Type an unused port number in the **Listen on Port** field and select **Apply**.

To change the SSL VPN port - CLI:

This is a global setting. For example, to set the SSL VPN port to 10443, enter:

```
config vpn ssl settings
   set port 10443
end
```

SSL offloading

To configure SSL offloading, which allows or denies client renegotiation, you must use the CLI. This helps to resolve the issues that affect all SSL and TLS servers that support renegotiation, identified by the Common Vulnerabilities and Exposures system in CVE-2009-3555. The SSL offloading renegotiation feature is considered a workaround until the IETF permanently resolves the issue.

The CLI command is `ssl-client-renegotiation` and is found under the `config firewall vip` syntax.

Host check

When you enable AV, FW, or AV-FW host checking in the web portal Security Control settings, each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can

create a custom host check that looks for security software selected from the Host Check list. For more information, see Additional configuration options on page 2173.

The Host Check list includes default entries for many security software products.

Host integrity checking is only possible with client computers running Microsoft Windows platforms.

To configure host checking - CLI:

To configure the full-access portal to check for AV and firewall software on client Windows computers, you would enter the following:

```
config vpn ssl web portal
   edit full-access
      set host-check av-fw
end
```

To configure the full-access portal to perform a custom host check for FortiClient Host Security AV and firewall software, you would enter the following:

```
config vpn ssl web portal
   edit full-access
      set host-check custom
      set host-check-policy FortiClient-AV FortiClient-FW
end
```

Replacing the host check error message

You can add your own host security check error message using either the web-based manager or the CLI. The default message reads: “Your PC does not meet the host checking requirements set by the firewall. Please check that your OS version or antivirus and firewall applications are installed and running properly or you have the right network interface.”

To replace the host check error message - web-based manager:

1. Navigate to **System > Config > Replacement Messages** and select **Extended View** in the upper right corner.
2. Scroll down to **SSL VPN** and select **Hostcheck Error Message**.
3. Edit the text in the right-hand column below and select **Save**.
   If you are unhappy with the new message, you can restore the message to its default by selecting **Restore Default** instead of **Save**.

To replace the host check error message - CLI:

Configure the host check error message using the following command.

```
config system replacemsg sslvpn hostcheck-error
```

Creating a custom host check list

You can add your own software requirements to the host check list using the CLI. Host integrity checking is only possible with client computers running Microsoft Windows platforms. Enter the following commands:

```
config vpn ssl web host-check-software
   edit <software_name>
```

```
        set guid <guid_value>
        set type <av | fw>
        set version <version_number>
    end
```

If known, enter the Globally Unique Identifier (GUID) for the host check application. Windows uses GUIDs to identify applications in the Windows Registry. The GUID can be found in the Windows registry in the HKEY_ CLASSES_ROOT section.

To obtain the exact versioning, in Windows, right-click on the .EXE file of the application and select **Properties**, then select the **Version** tab.

Host Check is applicable for both SSLVPN Web Mode and SSLVPN Tunnel mode.

Windows OS check

The Windows patch check enables you to define the minimum Windows version and patch level allowed when connecting to the SSL VPN portal. When the user attempts to connect to the web portal, FortiOS performs a query on the version of Windows the user has installed. If it does not match the minimum requirement, the connection is denied. The Windows patch check is configured in the CLI.

The following example shows you how to add an OS check to the 'g1portal' web portal. This OS check accepts all Windows XP users and Windows 2000 users running patch level 3.

To specify the acceptable patch level, you set the `latest-patch-level` and the `tolerance`. The lowest acceptable patch level is `latest-patch-level` minus `tolerance`. In this case, `latest-patch-level` is 3 and `tolerance` is 1, so 2 is the lowest acceptable patch level.

```
config vpn ssl web portal
   edit g1portal
      set os-check enable
      config os-check-list windows-2000
         set action check-up-to-date
         set latest-patch-level 3
         set tolerance 1
      end
      config os-check-list windows-xp
         set action allow
      end
   end
```

Host check for Windows firewall

The Windows built-in firewall does not have a GUID in root\securitycenter or root\securitycenter2, but you can use a registry value to detect the firewall status.

If Windows firewall is on, the following registry value will be set to 1:

- **KeyName:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\ FirewallPolicy\StandardProfile
- **ValueName:** EnableFirewall

In FortiOS, use the registry-value-check feature to define the Windows Firewall software by entering the following in the CLI:

```
config vpn ssl web host-check-software
   edit "Microsoft-Windows-Firewall"
      config check-item-list
         edit 1
```

```
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\StandardProfile:EnableFirewall==1"
            set type registry
         next
         edit 2
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\PublicProfile:EnableFirewall==1"
            set type registry
         next
         edit 3
            set target
                "HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\Firew
                allPolicy\\DomainProfile:EnableFirewall==1"
            set type registry
         next
      end
   set type fw
next
set host-check custom
set host-check-policy Microsoft-Windows-Firewall
```

Configuring cache cleaning

When the SSL VPN session ends, the client browser cache may retain some information. To enhance security, cache cleaning clears this information just before the SSL VPN session ends.

The cache cleaner is effective only if the session terminates normally. The cache is not cleaned if the session ends due to a malfunction, such as a power failure.

To enable cache cleaning

To enable cache cleaning on the full-access portal, you would enter:

```
config vpn ssl web portal
   edit full-access
      set cache-cleaner enable
   end
```

Cache cleaning requires a browser plugin. If the user does not have the plugin, it is automatically downloaded to the client computer.

Configuring virtual desktop

Available for 32-bit Windows XP, Windows Vista, and Windows 7 client PCs, the virtual desktop feature completely isolates the SSL VPN session from the client computer's desktop environment. All data is encrypted, including cached user credentials, browser history, cookies, temporary files, and user files created during the session. When the SSL VPN session ends normally, the files are deleted. If the session ends due to a malfunction, files might remain, but they are encrypted so that the information is protected.

When the user starts an SSL VPN session that has virtual desktop enabled, the virtual desktop replaces the user's normal desktop. When the virtual desktop exits, the user's normal desktop is restored.

Virtual desktop requires the Fortinet cache cleaner plugin. If the plugin is not present, it automatically downloads to the client computer.

To enable virtual desktop :

To enable virtual desktop on the full-access portal and apply the application control list 'List1', for example, you would enter:

```
config vpn ssl web portal
   edit full-access
      set virtual-desktop enable
      set virtual-desktop-app-list List1
   end
```

Configuring virtual desktop application control

You can control which applications users can run on their virtual desktop. To do this, you create an Application Control List of either allowed or blocked applications. When you configure the web portal, you select the list to use.

Configure the application control list in the CLI.

To create an Application Control List - CLI:

If you want to add 'BannedApp' to 'List1', a list of blocked applications, you would enter:

```
config vpn ssl web virtual-desktop-app-list
   edit "List1"
      set action block
      config apps
         edit "BannedApp"
            set md5s "06321103A343B04DF9283B80D1E00F6B"
         end
   end
```

Configuring client OS Check

The SSLVPN client OS Check feature can determine if clients are running the Windows 2000, Windows XP, Windows Vista or Windows 7 operating system. You can configure the OS Check to do any of the following:

- Allow the client access.
- Allow the client access only if the operating system has been updated to a specified patch (service pack) version.
- Deny the client access.

The OS Check has no effect on clients running other operating systems.

To configure OS Check:

OS Check is configurable only in the CLI.

```
config vpn ssl web portal
   edit <portal_name>
      set os-check enable
      config os-check-list {windows-2000 | windows-xp | windows-vista | windows-7}
         set action {allow | check-up-to-date | deny}
         set latest-patch-level {disable | 0 - 255}
         set tolerance {tolerance_num}
```

```
    end
  end
```

Adding WINS and DNS services for clients

You can specify the WINS or DNS servers that are made available to SSL-VPN clients.

DNS servers provide the IP addresses that browsers need to access web sites. For Internet sites, you can specify the DNS server that your FortiGate unit uses. If SSL VPN users will access intranet sites using URLs, you need to provide them access to the intranet's DNS server. You specify a primary and a secondary DNS server.

A WINS server provides IP addresses for named servers in a Windows domain. If SSL VPN users will access a Windows network, you need to provide them access to the domain WINS server. You specify a primary and a secondary WINS server.

To specify WINS and DNS services for clients - web-based manager:

1. Go to **VPN > SSL > Settings**.
2. Next to **DNS Server** select **Specify**.
3. Enter the IP addresses of DNS servers in the **DNS Server** fields as needed. Fields are available for both IPv4 and IPv6 addresses.
4. Select **Specify WINS Servers**, and enter the IP addresses of WINS servers in the **WINS Server** fields as needed. Fields are available for both IPv4 and IPv6 addresses.
5. Select **Apply**.

To specify WINS and DNS services for clients - CLI:

```
config vpn ssl settings
   set dns-server1 <address_ipv4>
   set dns-server2 <address_ipv4>
   set wins-server1 <address_ipv4>
   set wins-server2 <address_ipv4>
end
```

Setting the idle timeout setting

The idle timeout setting controls how long the connection can remain idle before the system forces the remote user to log in again. For security, keep the default value of 5000 seconds or less. Set the timeout value to 0 to disable idle timeouts.

To set the idle timeout - web-based manager:

1. Go to **VPN > SSL > Settings** and enable **Idle Logout**.
2. In the **Inactive For** field, enter the timeout value.
   The valid range is from 10 to 28800 seconds.
3. Select **Apply**.

To set the idle timeout - CLI:

```
config vpn ssl settings
   set idle-timeout <seconds_int>
end
```

SSL VPN logs

Logging is available for SSL VPN traffic so you can monitor users connected to the FortiGate unit and their activity. For more information on configuring logs on the FortiGate unit, see the Logging and Reporting Guide.

To enable logging of SSL VPN events - web-based manager:

1. Go to **Log & Report > Log Config > Log Settings**.
2. Enable **Event Logging**, and select **VPN activity event**.
3. Select **Apply**.

To view the SSL VPN log data, in the web-based manager, go to **Log & Report** and select either the **Event Log** or **Traffic Log**.

In event log entries, look for the sub-types “sslvpn-session” and “sslvpn-user”.

For information about how to interpret log messages, see the FortiGate Log Message Reference.

Monitoring active SSL VPN sessions

You can go to **User & Device > Monitor** to view a list of active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time the connection was made. You can also see which services are being provided, and delete an active web session from the FortiGate unit.

To monitor SSL VPNs - web-based manager:

To view the list of active SSL VPN sessions, go to **VPN > Monitor > SSL-VPN Monitor**.

When a tunnel-mode user is connected, the **Description** field displays the IP address that the FortiGate unit assigned to the remote host.

If required, you can end a session/connection by selecting its checkbox and then clicking the **Delete** icon.

Importing and using a CA-signed SSL certificate

Use the following set of instructions to import a CA-signed SSL certificate and configure an SSL VPN using that certificate.

Import the signed certificate into your FortiGate device

1. Unzip the file downloaded from the CA.
   There should be two .CRT files: a CA certificate with bundle in the file name, and a local certificate.
2. Log in to your FortiGate unit and browse to **System > Certificates**.
3. Select **Import > Local Certificate** to import the local certificate.
   The status of the certificate will change from PENDING to OK.
4. Import the CA certificate by selecting **Import > CA Certificate**.
   It will be listed in the CA Certificates section of the certificates list. You can now configure SSL VPN using the signed certificate.

Configure your FortiGate device to use the signed certificate

1. Log in to your FortiGate unit and browse to **VPN > SSL > Settings**.
2. In the **Connection Settings** section, locate the **Server Certificate** field.

3. Select the new certificate from the drop-down menu.
4. Select **Apply** to configure SSL VPN to use the new certificate.

The SSL VPN client

The remote client connects to the SSL VPN tunnel in various ways, depending on the VPN configuration.

- Web mode requires nothing more than a web browser. Microsoft Internet Explorer, Firefox, and Apple Safari browsers are supported. For detailed information about supported browsers, see Web-only mode on page 2150.
- Tunnel mode establishes a connection to the remote protected network that any application can use. If the client computer runs Microsoft Windows, they can download the tunnel mode client from the web portal Tunnel Mode widget. After installing the client, they can start and stop tunnel operation from the Tunnel Mode widget, or open the tunnel mode client as a standalone application. The tunnel mode client is available on the Start menu at **All Programs > FortiClient > FortiClient SSL VPN**.
  If the client computer runs Linux or Mac OS X, the user needs to download the tunnel mode client application from the Fortinet Support web site. See the Release Notes for your FortiOS firmware for the specific operating system versions that are supported. On Linux and Mac OS X platforms, tunnel mode operation cannot be initiated from the web portal Tunnel Mode widget. The remote user must use the standalone tunnel client application.
- The virtual desktop application creates a virtual desktop on a user's PC and monitors the data read/write activity of the web browser running inside the virtual desktop. When the application starts, it presents a 'virtual desktop' to the user. The user starts the web browser from within the virtual desktop and connects to the SSL VPN web portal. The browser file/directory operation is redirected to a new location, and the data is encrypted before it is written to the local disk. When the virtual desktop application exits normally, all the data written to the disk is removed. If the session terminates abnormally (power loss, system failure, etc.), the data left behind is encrypted and unusable to the user. The next time you start the virtual desktop, the encrypted data is removed.

FortiClient

Remote users can use the FortiClient software to initiate an SSL VPN tunnel to connect to the internal network. FortiClient uses local port TCP 1024 to initiate an SSL encrypted connection to the FortiGate unit, on port TCP 443. When connecting using FortiClient, the FortiGate unit authenticates the FortiClient SSL VPN request based on the user group options. The FortiGate unit establishes a tunnel with the client and assigns a virtual IP address to the client PC. Once the tunnel has been established, the user can access the network behind the FortiGate unit.

FortiClient software is available for download at www.forticlient.com and is available for Windows, Mac OS X, Apple iOS, and Android.

Tunnel mode client configuration

The FortiClient SSL VPN tunnel client requires basic configuration by the remote user to connect to the SSL VPN tunnel. When distributing the FortiClient software, provide the following information for the remote user to enter once the client software has been started. Once entered, they can select **Connect** to begin an SSL VPN session.

Connection Name	If you have pre-configured the connection settings, select the connection from the list and then select **Connect**. Otherwise, enter the settings in the fields below.
Remote Gateway	Enter the IP address or FQDN of the FortiGate unit that hosts the SSL VPN.
Username	Enter your username.
Client Certificate	Use this field if the SSL VPN requires a certificate for authentication. Select the required certificate from the drop-down list. The certificate must be installed in the Internet Explorer certificate store.

The SSL VPN web portal

This chapter explains how to use and configure the web portal features. This chapter is written for end users as well as administrators.

The following topics are included:

Connecting to the FortiGate unit
Web portal overview
Portal configuration
Using the My Bookmarks widget
Using the Connection Tool
Tunnel-mode features
Using the SSL VPN virtual desktop
Using FortiClient

Connecting to the FortiGate unit

You can connect to the FortiGate unit using a web browser. The URL of the FortiGate interface may vary from one installation to the next. If required, ask your FortiGate administrator for the URL of the FortiGate unit, and obtain a user name and password. You can connect to the web portal using an Android phone, iPhone, or iPad. The FortiGate unit will display the content of the portal to fit the device's screen.

In addition, if you will be using a personal or group security (X.509) certificate to connect to the FortiGate unit, your web browser may prompt you for the name of the certificate. Your FortiGate administrator can tell you which certificate to select.

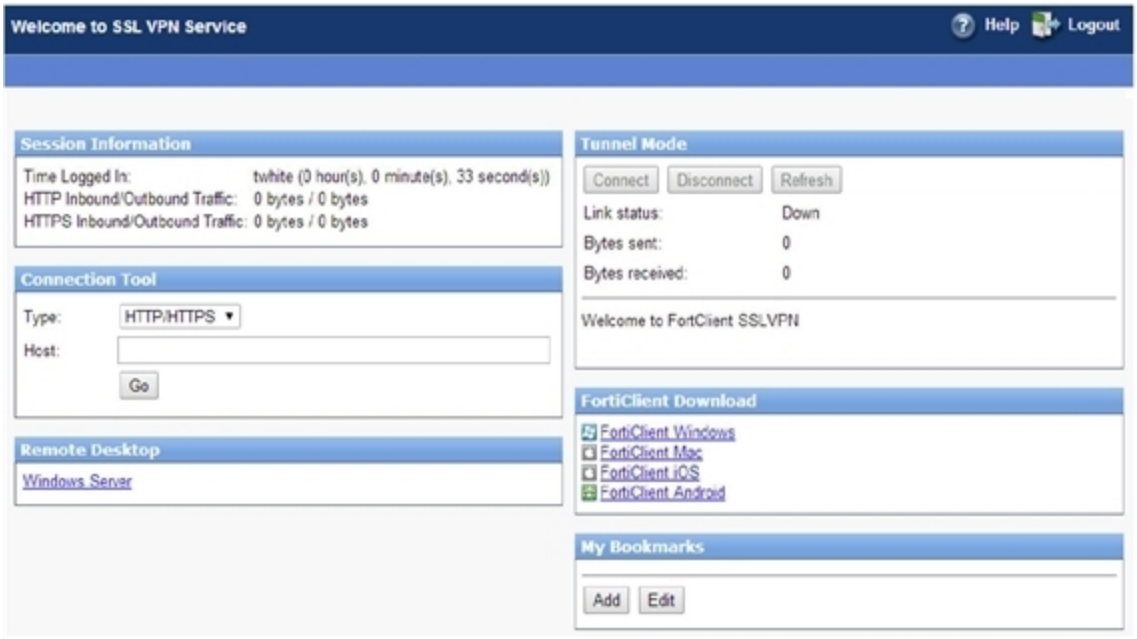
To log into the secure FortiGate HTTP gateway

1. Using the web browser on your computer, browse to the URL of the FortiGate unit (for example, `https://`<FortiGate_IP_address>`:443/remote/login`). The FortiGate unit may offer you a self-signed security certificate. If you are prompted to proceed, select **Yes**.
   A second message may be displayed to inform you that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. You can ignore the message.
2. When you are prompted for your user name and password:
   - In the **Name** field, type your user name.
   - In the **Password** field, type your password.
3. Select **Login**.
   The FortiGate unit will redirect your web browser to the FortiGate SSL VPN web portal home page automatically.

Web portal overview

After you log in, you see a web portal page like the following:

FortiGate SSL VPN web portal page



Six"widgets" provide the web portal's features:

- **Session Information** displays the elapsed time since login and the volume of HTTP and HTTPS traffic, both inbound and outbound.
- **Tunnel Mode** connects and disconnects the tunnel mode SSL connection to the FortiGate unit. While the tunnel is active, the widget displays the amount of data that is sent and received. For more information, see Web portal overview on page 2184.

  Tunnel mode requires a downloadable client application. If your computer is running Microsoft Windows, the Tunnel Mode widget provides a download link if you need to install the client on your computer. If you are using Macintosh or Linux, you can obtain and install an appropriate client application from the Fortinet Support site.
- **Connection Tool** enables you to connect to network resources without using or creating a bookmark.
- **Remote Desktop** provides access to preconfigured remote desktop environments.
- **FortiClient Download** provides access to the FortiClient tunnel application for various operating systems.
- **My Bookmarks** provides links to network resources. You can use the administrator-defined bookmarks and you can add your own bookmarks. See Web portal overview on page 2184.

Depending on the web portal configuration and user group settings, some widgets might not be present. For example, the predefined web-access portal contains only the Session Information and Bookmarks widgets.

While using the web portal, you can select the **Help** button to get information to assist you in using the portal features. This information displays in a separate browser window.

When you have finished using the web portal, select the **Logout** button in the top right corner of the portal window.

After making any changes to the web portal configuration, be sure to select **Apply**.

Portal configuration

The SSL VPN Service portal enables users to access network resources through a secure channel using a web browser. Fortinet administrators can configure log in privileges for system users and which network resources are available to the users.

The portal configuration determines what the user sees when they log in to the portal. Both the system administrator and the user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- **full-access**: Includes all widgets available to the user - **Session Information**, **Tunnel Mode**, **Connection Tool**, **FortiClient Download**, **Remote Desktop**, and **My Bookmarks**.
- **tunnel-access**: Includes **Session Information** and **Tunnel Mode** widgets.
- **web-access**: Includes **Session Information** and **My Bookmarks** widgets.

You can also create your own web portal to meet your corporate requirements.

This topic includes the following:

- Portal settings
- Portal widgets

Portal page	
Create New	Creates a new web portal.
Edit	Select a portal from the list to enable the Edit option, and modify the portal configuration.
Delete	Removes a portal configuration. To remove multiple portals from the list, select the check box beside the portal names, then select **Delete**.
Name	The name of the web portal.
Ref.	Displays the number of times the object is referenced in other configurations on the FortiGate unit, such as security policies. To view the location of the referenced object, select the number in **Ref.** column. To view more information about how the object is used, select one of: **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. **Edit this object** – modifies settings within that particular setting that the object is referenced with. **View the details for this object** – similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with.
Portal Settings page	
Edit Settings window	Provides general, virtual desktop and security control settings for the SSL VPN Service portal page. This window appears when you select **Settings**. This window also appears whenever you select **Create New** and are automatically redirected to the Portal Settings page. For more information, see Portal settings on page 2188.
Settings	Select to edit the settings for the SSL VPN web portal. See Portal configuration on page 2186.
Widgets	The widgets that will appear on the SSL VPN Service page. You can add widgets from the Add Widgets drop-down list. For more information, see Portal widgets on page 2191.
Add Widget	Select to add a new widget to the page.

Session Information	Displays basic information of the current session of the logged in user. For more information, see Session Information on page 2191.
Bookmarks	Displays configured bookmarks, allows for the addition of new bookmarks and editing of existing bookmarks. For more information, see Bookmarks on page 2191.
Connection Tool	Enter the URL or IP address for a connection tool application/server (selected when configuring the **Connection Tool**). You can also check connectivity to a host or server on the network behind the unit by selecting the **Type** Ping. For more information, see Connection Tool on page 2191.
Tunnel Mode	Displays tunnel information and actions in user mode. The administrator can configure a split-tunneling option. For more information, see Tunnel Mode on page 2191.

Portal settings

A web portal defines SSL VPN user access to network resources. The portal configuration determines what SSL VPN users see when they log in to the unit. Both the Fortinet administrator and the SSL VPN user have the ability to customize the web portal settings. Portal settings are configured in **VPN > SSL > Portals**.

The Settings Window provides settings for configuring general, virtual desktop and security console options for your web portal.

The virtual desktop options, available for Windows XP and Windows Vista client PCs, are configured to completely isolate the SSL VPN session from the client computer's desktop environment. All data is encrypted, including cached user credentials, browser history, cookies, temporary files, and user files created during the session. When the SSL VPN session ends normally, the files are deleted. If the session ends unexpectedly, any files that may remain will be encrypted.

Virtual desktop requires the Fortinet host check plugin. If the plugin is not present, it is automatically downloaded to the client computer.

Security control options provide cache cleaning and host checking to the clients of your web portal. Cache cleaning clears information from the client browser cache just before the SSL VPN session ends. The cache cleaner is effective only if the session terminates normally. The cache is not cleaned if the session ends unexpectedly.

Host checking enforces the client's use of antivirus or firewall software. Each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for specific security software selected from the Host Check list. For more information, see Basic configuration on page 2155.

Edit Settings Window

General tab	
Name	Enter a name for the web portal configuration.
Applications	Select the server applications or network services clients can use.
Portal Message	Enter the caption that appears at the top of the web portal home page when the user logs in.
Theme	Select the color scheme for the web portal home page.
Page Layout	Select the one or two page column format for the web portal home page.
Redirect URL	Enter the URL that the web portal displays when the web portal home page is displayed.
Virtual Desktop tab	
Enable Virtual Desktop	Select to enable the virtual desktop.
Allow switching between virtual desktop and regular desktop	Select to allow users to switch between the virtual desktop, and their regular desktop.
Allow clipboard contents to be shared with regular desktop	Select to allow users access to the clipboard contents when they are using the regular desktop.
Allow use of removable media	Select to allow users to access removable media.
Allow network share access	Select to allow users to have access to network resources.
Allow printing	Select to allow users to print from the virtual desktop.
Quit the virtual desktop and logout session when browser is closed	Select to have the virtual desktop close and log the user out of the current session whenever the browser is closed.
Application Control List	Select a virtual desktop application list from the drop-down list.
Security Control tab	
Clean Cache	Select to have the unit remove residual information from the remote client computer just before the SSL VPN session closes.

Host Check	Select any host checking that is required before the user can log into the portal. Host checks will verify if the user has the required antivirus software or applications. If the user does not, the log in will be denied. Host Check is applicable for both SSLVPN Web Mode and SSLVPN Tunnel mode. For more information, see Basic configuration on page 2155.
Interval	Enter how often to recheck the host for updates and changes in seconds.
Policy	This is available when the **Host Check selection is Custom**. Select the specific host check software to look for. Select **Edit** to modify the policy settings.

Portal widgets

Portal widgets are widgets hold the content the user logging into the portal will see.

Session Information

The **Session Information** widget displays the login name of the user, the amount of time the user has been logged in and the inbound and outbound traffic statistics.

Bookmarks

Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a pop-up window appears with the requested web page. Telnet, VNC, and RDP all pop up a window that requires a browser plug-in. FTP and Samba replace the bookmarks page with an HTML file-browser.

A web bookmark can include login credentials to automatically log the SSL VPN user into the web site. When the administrator configures bookmarks, the web site credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the web site.

Connection Tool

Use the **Connection Tool** widget to connect to a network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.

Tunnel Mode

If your web portal provides tunnel mode access, you need to configure the **Tunnel Mode** widget. These settings determine how tunnel mode clients are assigned IP addresses. You can also enable a split tunneling configuration so that the VPN carries only the traffic for the networks behind the unit. The user's other traffic follows its normal route.

Applications available in the web portal

Depending on the web portal configuration and user group settings, one or more of the following server applications are available to you through Bookmarks or the Connection Tool:

- Citrix makes use of SOCKS so that the Citrix client can connect to the SSL VPN port forward module to provide the connection.
- FTP (File Transfer Protocol) enables you to transfer files between your computer and a remote host.
- HTTP/HTTPS accesses web pages.
- Port Forward provides the middle ground between web mode and tunnel mode. When the SSL VPN receives data from a client application, the data is encrypted and sent to the FortiGate unit, which then forwards the traffic to the application server.
- RDP/RDP Native (Remote Desktop Protocol), similar to VNC, enables you to remotely control a computer running Microsoft Terminal Services.
- SMB/CIFS implements the Server Message Block (SMB) protocol to support file sharing between your computer and a remote server host.
- SSH (Secure Shell) enables you to exchange data between two computers using a secure channel.
- TELNET (Teletype Network emulation) enables you to use your computer as a virtual text-only terminal to log in to a remote host.
- VNC (Virtual Network Computing) enables you to remotely control another computer, for example, accessing your work computer from your home computer.

Some server applications may prompt you for a user name and password. You must have a user account created by the server administrator so that you can log in.

RDP Native, in some instances, may not be supported. If this is the case, use Internet Explorer and disable ActiveX Filtering.

Windows file sharing through SMB/CIFS is supported through shared directories.

Using the My Bookmarks widget

The My Bookmarks widget shows both administrator-configured and user-configured bookmarks. Administrator bookmarks cannot be altered but you can add, edit or delete user bookmarks.

My Bookmarks widget

The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the My Bookmarks list. For more information, see Adding bookmarks on page 2193.

If you want to access a web server or telnet server without first adding a bookmark to the My Bookmarks list, use the Connection Tool instead. For more information, see Using the My Bookmarks widget on page 2192.

Adding bookmarks

You can add frequently used connections as bookmarks. Afterward, select any hyperlink from the Bookmarks list to initiate a session.

To add a bookmark

1. In the **Bookmarks** widget, select **Add**.
2. Enter the following information:

Name	Enter the name to display in the Bookmarks list.
Type	Select the abbreviated name of the server application or network service from the drop-down list.
Location	Enter the IP address or FQDN of the server application or network service. For RDP connections, you can append some parameters to control screen size and keyboard layout. See Using the My Bookmarks widget on page 2192.
Description	Optionally enter a short description. The description displays when you pause the mouse pointer over the hyperlink.
SSO	Single Sign On (SSO) is available for HTTP/HTTPS bookmarks only. **Disabled** — This is not an SSO bookmark. **Automatic** — Use your SSL VPN credentials or an alternate set. See the **SSO Credentials** field. **Static** — Supply credentials and other required information (such as an account number) to a web site that uses an HTML form for authentication. You provide a list of the form field names and the values to enter into them. This method does not work for sites that use HTTP authentication, in which the browser opens a pop-up dialog box requesting credentials.
SSO fields	
SSO Credentials	**SSL VPN Login** — Use your SSL VPN login credentials. **Alternative** — Enter **Username** and **Password** below.
Username	Alternative username. Available if **SSO Credentials** is **Alternative**.

Password	Alternative password. Available if **SSO Credentials** is **Alternative**.
Static SSO fields	These fields are available if **SSO** is **Static**.
Field Name	Enter the field name, as it appears in the HTML form.
Value	Enter the field value. To use the values from **SSO Credentials**, enter `%passwd%` for password or `%username%` for username.
Add	Add another **Field Name** / **Value** pair.

3. Select **OK** and then select **Done**.

Using the Connection Tool

The **Connection Tool** widget enables a user to connect to a resource when it isn't a bookmark. In the FortiGate, ensure that the desired application or protocol (to which you want remote users to connect) is enabled in the **Applications** list of the **General** settings, by selecting the **Settings** button in the portal configuration window.

You can connect to any type of server without adding a bookmark to the My Bookmarks list. The fields in the Connection Tool enable you to specify the type of server and the URL or IP address of the host computer.

See the following procedures:

- To connect to a web server on page 2194
- To ping a host or server behind the FortiGate unit on page 2195
- To start a Telnet session on page 2195
- To start an FTP session on page 2195
- To start an SMB/CIFS session on page 2195
- To start an SSH session on page 2196
- To start an RDP session on page 2196
- To start a VNC session on page 2197

Except for ping, these services require that you have an account on the server to which you connect.

When you use the Connection Tool, the FortiGate unit may offer you its self-signed security certificate. Select **Yes** to proceed. A second message may be displayed to inform you of a host name mismatch. This message is displayed because the FortiGate unit is attempting to redirect your web browser connection. Select **Yes** to proceed.

To connect to a web server

1. In **Type**, select **HTTP/HTTPS**.
2. In the **Host** field, type the URL of the web server.
   For example: `http://www.mywebexample.com` or `https://172.20.120.101`
3. Select **Go**.
4. To end the session, close the browser window.

To ping a host or server behind the FortiGate unit

1. In **Type**, select **Ping**.
2. In the **Host** field, enter the IP address of the host or server that you want to reach.
   For example: `10.11.101.22`
3. Select **Go**.
   A message stating whether the IP address can be reached or not is displayed.

To start a Telnet session

1. In **Type**, select **Telnet**.
2. In the **Host** field, type the IP address of the telnet host.
   For example: `10.11.101.12`
3. Select **Go**.
   A Telnet window opens.
4. Select **Connect**.
5. A telnet session starts and you are prompted to log in to the remote host.
   After you log in, you may enter any series of valid telnet commands at the system prompt.
6. To end the session, select **Disconnect** (or type `exit`) and then close the TELNET connection window.

To start an FTP session

1. In **Type**, select **FTP**.
2. In the **Host** field, type the IP address of the FTP server.
   For example: `10.11.101.12`
3. Select **Go**.
   A login window opens.
4. Enter your user name and password and then select **Login**.
   You must have a user account on the remote host to log in.
5. Manipulate the files in any of the following ways:
   - To download a file, select the file link in the **Name** column.
   - To access a subdirectory (**Type** is **Folder**), select the link in the **Name** column.
   - To create a subdirectory in the current directory, select **New directory**.
   - To delete a file or subdirectory from the current directory, select its **Delete** icon.
   - To rename a file in the current directory, select its **Rename** icon.
   - To upload a file to the current directory from your client computer, select **Upload**.
   - When the current directory is a subdirectory, you can select **Up** to access the parent directory.
6. To end the FTP session, select **Logout**.

To start an SMB/CIFS session

1. In **Type**, select **SMB/CIFS**.
2. In the **Host** field, type the IP address of the SMB or CIFS server.
   For example: `10.11.101.12`
3. Select **Go**.
4. Enter your user name and password and then select **Login**.

You must have a user account on the remote host to log in.

5. Manipulate the files in any of the following ways:
   - To download a file, select the file link in the **Name** column.
   - To access a subdirectory (**Type** is **Folder**), select the file link in the **Name** column.
   - To create a subdirectory in the current directory, select **New Directory**.
   - To delete a file or subdirectory from the current directory, select its **Delete** icon.
   - To rename a file, select its **Rename** icon.
   - To upload a file from your client computer to the current directory, select **Upload**.
   - When the current directory is a subdirectory, you can select **Up** to access the parent directory.
6. To end the SMB/CIFS session, select **Logout** and then close the SMB/CIFS window.

To start an SSH session

1. In **Type**, select **SSH**.
2. In the **Host** field, type the IP address of the SSH host.
   For example: `10.11.101.12`
3. Select **Go**.
   A login window opens.
4. Select **Connect**.
   A SSH session starts and you are prompted to log in to the remote host. You must have a user account to log in. After you log in, you may enter any series of valid commands at the system prompt.
5. To end the session, select **Disconnect** (or type `exit`) and then close the SSH connection window.

To start an RDP session

1. In **Type**, select **RDP**.
2. In the **Host** field, type the IP address of the RDP host.
   For example: `10.11.101.12`
3. Optionally, you can specify additional options for RDP by adding them to the **Host** field following the host address. See RDP options on page 2196 for information about the available options.
   For example, to use a French language keyboard layout you would add the `-m` parameter:
   `10.11.101.12 -m fr`
4. Select **Go**.
   A login window opens.
5. When you see a screen configuration dialog, click **OK**.
   The screen configuration dialog does not appear if you specified the screen resolution with the host address.
6. When you are prompted to log in to the remote host, type your user name and password. You must have a user account on the remote host to log in.
7. Select **Login**.
   If you need to send Ctrl-Alt-Delete in your session, use Ctrl-Alt-End.
8. To end the RDP session, Log out of Windows or select **Cancel** from the Logon window.

RDP options

When you specify the RDP server address, you can also specify other options for your remote desktop session.

Screen resolution Use this command to make the RDP window full screen or a specific the window size.	`-f` Make RDP full-screen `-g <width>x<height>` `<width>` and `<height>` are in pixels Example: `-g 800x600`

Authentication
 	
Use these options to send your authentication credentials with the connection request, instead of entering them after the connection is established.
	`-u <user name>`
	`-p <password>`
	`-d <domain>`

Locale/Keyboard Use this option if the remote computer might not use the same keyboard layout as your computer. Select the locale code that matches your computer.	-m <locale> The supported values of `<locale>` are:

ar	Arabic	it	Italian
da	Danish	ja	Japanese
de	German	lt	Lithuanian
de-ch	Swiss German	lv	Latvian
en-gb	British English	mk	Macedonian
en-uk	UK English	no	Norwegian
en-us	US English	pl	Polish
es	Spanish	pt	Portuguese
fi	Finnish	pt-br	Brazilian Portuguese
fr	French	ru	Russian
fr-be	Belgian French	sl	Slovenian
fr-ca	Canadian French	sv	Sudanese
fr-ch	Swiss French	tk	Turkmen
hr	Croatian	tr	Turkish
hu	Hungarian		

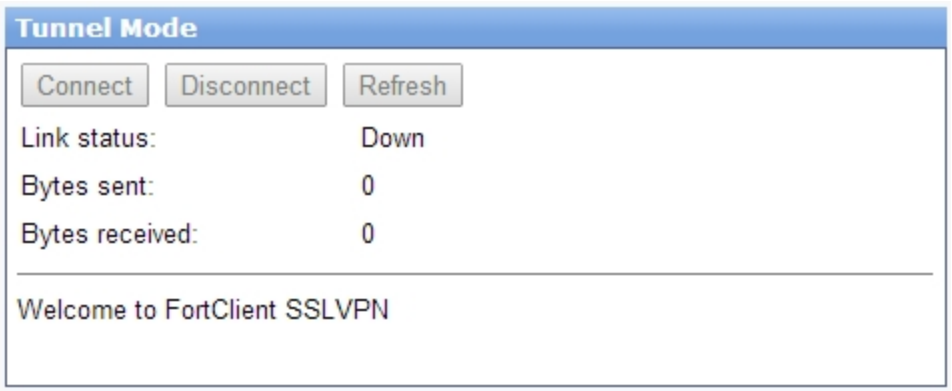
To start a VNC session

1. In **Type**, select **VNC**.
2. In the **Host** field, type the IP address of the VNC host.
   For example: `10.11.101.12`
3. Select **Go**.
   A login window opens.
4. Type your user name and password when prompted to log in to the remote host.
   You must have a user account on the remote host to log in.
5. Select **OK**.
   If you need to send Ctrl-Alt-Delete in your session, press F8, then select **Send Ctrl-Alt-Delete** from the pop-up menu.
6. To end the VNC session, close the VNC window.

Tunnel-mode features

For Windows users, the web portal Tunnel Mode widget provides controls for your tunnel mode connection and also provides status and statistics about its operation. You can also control and monitor tunnel mode operation from the standalone client application.

Fortinet SSL VPN Tunnel Mode widget



Connect	Initiate a session and establish an SSL VPN tunnel with the FortiGate unit.
Disconnect	End the session and close the tunnel to the FortiGate unit.
Refresh	Refresh the status and statistics immediately.
Link Status	The state of the SSL VPN tunnel: **Up** — an SSL VPN tunnel with the FortiGate unit has been established. **Down** — a tunnel connection has not been initiated.
Bytes Sent	The number of bytes of data transmitted from the client to the FortiGate unit since the tunnel was established.
Bytes Received	The number of bytes of data received by the client from the FortiGate unit since the tunnel was established.

Using the SSL VPN virtual desktop

The virtual desktop feature is available for Windows only. When you start an SSL VPN session, the virtual desktop replaces your normal desktop. When the virtual desktop exits, your regular desktop is restored. Virtual desktop information is encrypted so that no information from it remains available after your session ends.

To use the SSL VPN virtual desktop, simply log in to an SSL VPN that requires the use of the virtual desktop. Wait for the virtual desktop to initialize and replace your desktop with the SSL VPN desktop, which has a Fortinet SSL VPN logo as wallpaper. Your web browser will open to the web portal page.

You can use the virtual desktop just as you use your regular desktop, subject to the limitations that virtual desktop application control imposes. If it is enabled in the web portal virtual desktop settings, you can switch between the virtual desktop and your regular desktop. Right-click the **SSL VPN Virtual Desktop** icon in the taskbar and select **Switch Desktop**.

To see the web portal virtual desktop settings, right-click the **SSL VPN Virtual Desktop** icon in the taskbar and select **Virtual Desktop Option**.

When you have finished working with the virtual desktop, right-click the SSL VPN Virtual Desktop icon in the taskbar and select **Exit**. Select **Yes** to confirm. The virtual desktop closes and your regular desktop is restored.

Using FortiClient

Remote users can use FortiClient Endpoint Security to initiate an SSL VPN tunnel to connect to the internal network. FortiClient uses local port TCP 1024 to initiate an SSL encrypted connection to the FortiGate unit, on port TCP 10443. When connecting using FortiClient, the FortiGate unit authenticates the FortiClient SSL VPN request based on the user group options. the FortiGate unit establishes a tunnel with the client and assigns a virtual IP address to the client PC. Once the tunnel has been established, the user can access the network behind the FortiGate unit.

For information on configuring the FortiGate unit for SSL VPN connectivity, see Basic configuration on page 2155. For details on configuring FortiClient for SSL VPN connections, see the FortiClient documentation.

Setup examples

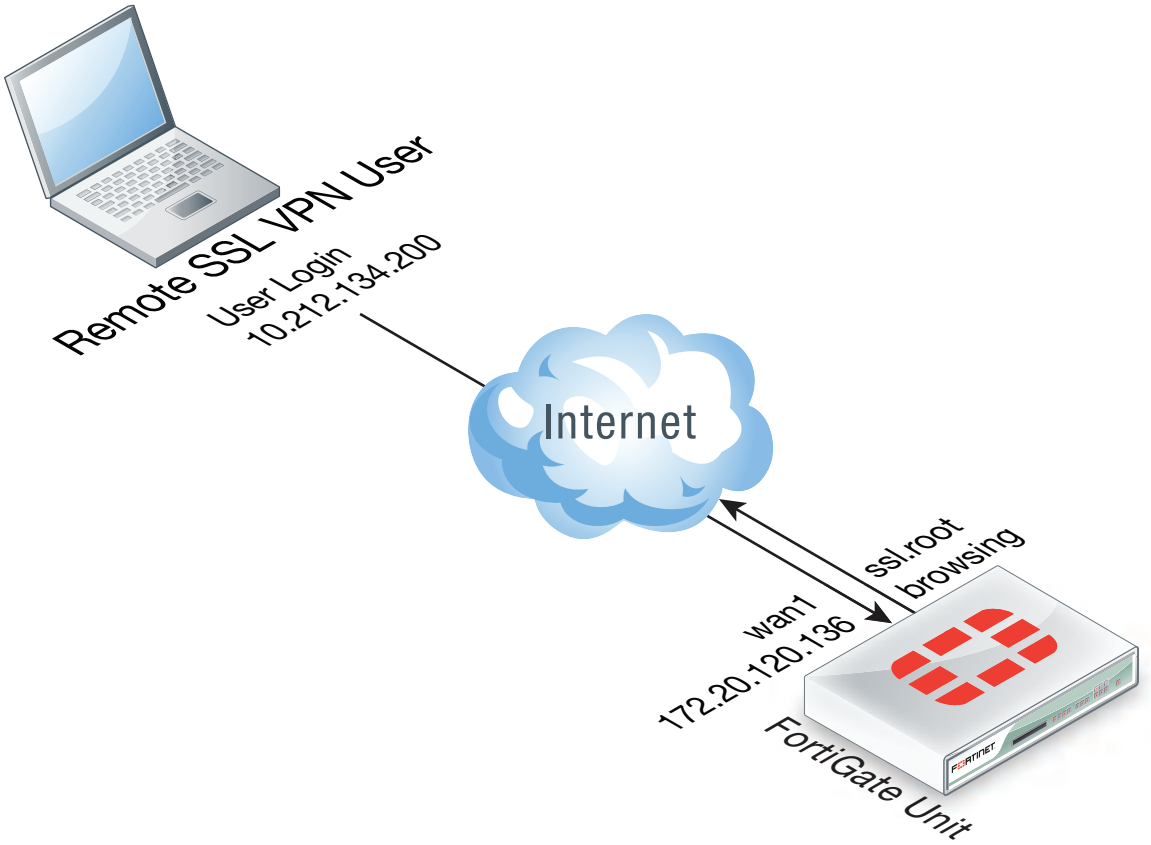
The examples in this chapter demonstrate the basic configurations needed for common connections to the SSL VPN tunnel and portals, applying the steps outlined in Basic configuration on page 2155.

The following examples are included:

Secure Internet browsing
Split Tunnel
Multiple user groups with different access permissions

Secure Internet browsing

This example sets up an SSL VPN tunnel that provides remote users the ability to access the Internet while traveling, and ensures that they are not subject to malware and other dangers, by using the corporate firewall to filter all of their Internet traffic. Essentially, the remote user will connect to the corporate FortiGate unit to surf the Internet.



Using SSL VPN and FortiClient SSL VPN software, you create a means to use the corporate FortiGate to browse the Internet safely.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to **VPN > SSL > Portals** and select *tunnel-access*.
2. For **Source IP Pools** select **SSLVPN_TUNNEL_ADDR1**.
3. Select **OK**.

Creating the SSL VPN user and user group

1. Create the SSL VPN user and add the user to a user group configured for SSL VPN use.
2. Go to **User & Device > User > User Definition** and select **Create New** to add the user:

User Name	twhite
Password	password

3. Select **OK**.
4. Go to **User & Device > User > User Groups** and select **Create New** to add `twhite` to a group called `SSL VPN`:

Name	SSL VPN
Type	Firewall

5. Move **twhite** to the **Members** list.
6. Select **OK**.

Creating a static route for the remote SSL VPN user

Create a static route to direct traffic destined for tunnel users to the SSL VPN tunnel.

1. Go to **Router > Static > Static Routes** and select **Create New** to add the static route.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.

Destination IP/Mask	10.212.134.0/255.255.255.0
Device	ssl.root

The **Destination IP/Mask** matches the network address of the remote SSL VPN user.

2. Select **OK**.

Creating security policies

Create an SSL VPN security policy with SSL VPN user authentication to allow SSL VPN traffic to enter the FortiGate unit. Create a normal security policy from ssl.root to wan1 to allow SSL VPN traffic to connect to the Internet.

Users and user groups are added to the SSL VPN under **VPN > SSL > Settings**, by adding a rule to the Authentication/Portal Mapping section. However, you must also add these users and user groups to the SSL VPN security policy.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Add an SSL VPN security policy as below, and click *OK*.

Incoming Interface	wan1
Source Address	all
Source User(s)	SSL VPN
Outgoing Interface	ssl.root

3. Select **Create New** to add a security policy that allows remote SSL VPN users to connect to the Internet:

Incoming Interface	ssl.root
Source Address	all
Source User(s)	SSL VPN
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

4. Select **OK**.

Configuring authentication rules

1. Go to **VPN > SSL > Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the remote user:

Users/Groups	Tunnel
Portal	tunnel-access

3. Select **OK** and **Apply**.

Results

Using the FortiClient SSLVPN application, access the VPN using the address `https://172.20.120.136:443/` and log in as `twhite`. Once connected, you can browse the Internet.

From the FortiGate web-based manager, go to **VPN > Monitor > SSL-VPN Monitor** to view the list of users connected using SSL VPN. The **Subsession** entry indicates the split tunnel which redirects to the Internet.

Split Tunnel

In this configuration, remote users are able to securely access the head office internal network through the head office firewall, yet browse the Internet without going through the head office FortiGate. Split tunneling is enabled by default for SSL VPN on FortiGate units.

The solution below describes how to configure FortiGate SSL VPN split tunneling using the FortiClient SSL VPN software, available from the Fortinet Support site.

Without split tunneling, all communication from remote SSL VPN users to the head office internal network and to the Internet uses an SSL VPN tunnel between the user's PC and the head office FortiGate unit. Connections to the Internet are routed back out the head office FortiGate unit to the Internet. Replies come back into the head office FortiGate unit before being routed back through the SSL VPN tunnel to the remote user.

In short, enabling split tunneling protects the head office from potentially harmful access and external threats that may occur as a result of the end user's indiscretion while browsing the Internet. By contrast, disabling split tunneling protects the end user by forcing all their Internet traffic to pass through the FortiGate firewall.

Creating a firewall address for the head office server

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New** and add the head office server address:

Category	Address
Name	Head office server
Type	Subnet
Subnet / IP Range	192.168.1.12
Interface	Internal

2. Select **OK**.

Creating an SSL VPN IP pool and SSL VPN web portal

1. Go to **VPN > SSL > Portals** and select **tunnel-access**.
2. Enter the following:

Name	Connect to head office server
Enable Tunnel Mode	Enable
Enable Split Tunneling	Enable
Routing Address	Internal
Source IP Pools	SSLVPN_TUNNEL_ADDR1

3. Select **OK**.

Creating the SSL VPN user and user group

Create the SSL VPN user and add the user to a user group.

1. Go to **User & Device > User > User Definition**, select **Create New** and add the user:

User Name	twhite
Password	password

2. Select **OK**.
3. Go to **User & Device > User > User Groups** and select **Create New** to add the new user to the SSL VPN user group:

Name	Tunnel
Type	Firewall

4. Move **twhite** to the **Members** list.
5. Select **OK**.

Creating a static route for the remote SSL VPN user

Create a static route to direct traffic destined for tunnel users to the SSL VPN tunnel.

1. Go to **Router > Static > Static Routes** and select **Create New**
2. For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**:

Destination IP/Mask	10.212.134.0/255.255.255.0
Device	ssl.root

3. Select **OK**.

Creating security policies

Create an SSL VPN security policy with SSL VPN user authentication to allow SSL VPN traffic to enter the FortiGate unit. Create a normal security policy from ssl.root to wan1 to allow SSL VPN traffic to connect to the Internet.

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Complete the following:

Incoming Interface	ssl.root
Source Address	all
Source User(s)	Tunnel
Outgoing Interface	internal
Destination Address	Head office server

3. Select **OK**.
4. Add a security policy that allows remote SSL VPN users to connect to the Internet.
5. Select **Create New**.
6. Complete the following and select **OK**:

Incoming Interface	ssl.root
Source Address	all
Source User(s)	Tunnel
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Configuring authentication rules

1. Go to **VPN > SSL > Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the remote user:

Users/Groups	Tunnel
Portal	tunnel-access

3. Select **OK** and **Apply**.

Results

Using the FortiClient SSL VPN application on the remote PC, connect to the VPN using the address `https://172.20.120.136:443/` and log in with the `twhite` user account. Once connected, you can connect to the head office server or browse to web sites on the Internet.

From the web-based manager, go to **VPN > Monitor > SSL-VPN Monitor** to view the list of users connected using SSL VPN. The **Subsession** entry indicates the split tunnel which redirects SSL VPN sessions to the Internet.

Multiple user groups with different access permissions

You might need to provide access to several user groups with different access permissions. Consider the following example topology in which users on the Internet have controlled access to servers and workstations on private networks behind a FortiGate unit.

In this example configuration, there are two users:

- User1 can access the servers on Subnet_1.
- User2 can access the workstation PCs on Subnet_2.

You could easily add more users to either user group to provide them access to the user group's assigned web portal.

General configuration steps

1. Create firewall addresses for:
   - The destination networks.
   - Two non-overlapping tunnel IP address ranges that the FortiGate unit will assign to tunnel clients in the two user groups.
2. Create two web portals.
3. Create two user accounts, User1 and User2.
4. Create two user groups. For each group, add a user as a member and select a web portal. In this example, User1 will belong to Group1, which will be assigned to Portal1 (similar configuration for User2).
5. Create security policies:
   - Two SSL VPN security policies, one to each destination.
   - Two tunnel-mode policies to allow each group of users to reach its permitted destination network.
6. Create the static route to direct packets for the users to the tunnel.

Creating the firewall addresses

Security policies do not accept direct entry of IP addresses and address ranges. You must define firewall addresses in advance.

Creating the destination addresses

SSL VPN users in this example can access either Subnet_1 or Subnet_2.

To define destination addresses - web-based manager:

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**, enter the following information, and select **OK**:

Name	Subnet_1
Type	Subnet
Subnet/IP Range	10.11.101.0/24
Interface	port2

3. Select **Create New**, enter the following information, and select **OK**:

Name	Subnet_2
Type	Subnet
Subnet/IP Range	10.11.201.0/24
Interface	port3

Creating the tunnel client range addresses

To accommodate the two groups of users, split an otherwise unused subnet into two ranges. The tunnel client addresses must not conflict with each other or with other addresses.

To define tunnel client addresses - web-based manager:

1. Go to **Policy & Objects > Objects > Addresses.**
2. Select **Create New**, enter the following information, and select **OK**:

Name	Tunnel_group1
Type	IP Range
Subnet/IP Range	10.11.254.1-10.11.254.50
Interface	Any

3. Select **Create New**, enter the following information, and select **OK**.

Name	Tunnel_group2
Type	IP Range
Subnet/IP Range	10.11.254.51-10.11.254.100
Interface	Any

Creating the web portals

To accommodate two different sets of access permissions, you need to create two web portals, portal1 and portal2, for example. Later, you will create two SSL VPN user groups, one to assign to portal1 and the other to assign to portal2.

To create the portal1 web portal:

1. Go to **VPN > SSL > Portals** and select **Create New**.
2. Enter `portal1` in the **Name** field.
3. In **Source IP Pools**, select **Tunnel_ group1**.
4. Select **OK**.

To create the portal2 web portal:

1. Go to **VPN > SSL > Portals** and select **Create New**.
2. Enter `portal2` in the **Name** field and select **OK**.
3. In **IP Pools**, select **Tunnel_ group2**
4. Select **OK**.

Later, you can configure these portals with bookmarks and enable connection tool capabilities for the convenience of your users.

Creating the user accounts and user groups

After enabling SSL VPN and creating the web portals that you need, you need to create the user accounts and then the user groups that require SSL VPN access.

Go to **User & Device > User > User Definition** and create user1 and user2 with password authentication. After you create the users, create the SSL VPN user groups.

To create the user groups - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select **Create New** and enter the following information:

Name	Group1
Type	Firewall

3. From the **Available** list, select **User1** and move it to the **Members** list by selecting the right arrow button.
4. Select **OK**.
5. Repeat steps 2 through 4 to create Group2, assigned to Portal2, with User2 as its only member.

Creating the security policies

You need to define security policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit. Before you create the security policies, you must define the source and destination addresses to include in the policy. See Creating the firewall addresses on page 2206.

Two types of security policy are required:

- An SSL VPN policy enables clients to authenticate and permits a web-mode connection to the destination network. In this example, there are two destination networks, so there will be two SSL VPN policies. The authentication ensures that only authorized users can access the destination network.
- A tunnel-mode policy is a regular ACCEPT security policy that enables traffic to flow between the SSL VPN tunnel interface and the protected network. Tunnel-mode policies are required if you want to provide tunnel-mode connections for your clients. In this example, there are two destination networks, so there will be two tunnel-mode policies.

To create the SSL VPN security policies - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New.**
2. Enter the following information and click **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	All
Source User(s)	Group1
Outgoing Interface	port2
Destination Address	Subnet_1
Service	All

3. Select **Create New.**
4. Enter the following information:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	All
Source User(s)	Group2
Outgoing Interface	port3
Destination Address	Subnet_2
Service	All

5. Click **OK**.

Configuring authentication rules

1. Go to **VPN > SSL > Settings** and select **Create New** under **Authentication/Portal Mapping**.
2. Add an authentication rule for the first remote group:

Users/Groups	Group1
Portal	Portal1

3. Select **OK** and **Apply**.
4. Select **Create New** and add an authentication rule for the second remote group:

Users/Groups	Group2
Portal	Portal2

5. Select **OK** and **Apply**.

To create the tunnel-mode security policies - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information, and select **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	Tunnel_group1
Source User(s)	Group1
Outgoing Interface	port2
Destination Address	Subnet_1
Service	All

Action	ACCEPT
Enable NAT	Enable

3. Select **Create New.**
4. Enter the following information, and select **OK**:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	Tunnel_group2
Source User(s)	Group2
Outgoing Interface	port3
Destination Address	Subnet_2
Service	All
Action	ACCEPT
Enable NAT	Enable

Create the static route to tunnel mode clients

Reply packets destined for tunnel mode clients must pass through the SSL VPN tunnel. You need to define a static route to allow this.

To add a route to SSL VPN tunnel mode clients - web-based manager:

1. Go to **Router > Static > Static Routes** and select **Create New**.

   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Enter the following information and select **OK**.

Destination IP/Mask	`10.11.254.0/24` This IP address range covers both ranges that you assigned to SSL VPN tunnel-mode users. See Creating the tunnel client range addresses on page 2207.
Device	Select the SSL VPN virtual interface, **ssl.root** for example.

In this example, the **IP Pools** field on the **VPN > SSL > Settings** page is not used because each web portal specifies its own tunnel IP address range.

Troubleshooting

This section contains tips to help you with some common challenges of SSL VPNs.

- Enter the following to display debug messages for SSL VPN:

  ```
  diagnose debug application sslvpn -1
  ```

  This command enables debugging of SSL VPN with a debug level of -1. The -1 debug level produces detailed results.

- Enter the following command to verify the debug configuration:

  ```
  diagnose debug info
  debug output: disable
  console timestamp: disable
  console no user log message: disable
  sslvpn debug level: -1 (0xffffffff)
  CLI debug level: 3
  ```

  This output verifies that SSL VPN debugging is enabled with a debug level of -1, and shows what filters are in place. The output above indicates that debug output is disabled, so debug messages are not displayed. The output also indicates that debugging has not been enabled for any software systems.

- Enter the following to enable displaying debug messages:

  ```
  diagnose debug enable
  ```

  To view the debug messages, log into the SSL VPN portal. The CLI displays debug output similar to the following:

  ```
  FGT60C3G10002814 # [282:root]SSL state:before/accept initialization (172.20.120.12)
  [282:root]SSL state:SSLv3 read client hello A (172.20.120.12)
  [282:root]SSL state:SSLv3 write server hello A (172.20.120.12)
  [282:root]SSL state:SSLv3 write change cipher spec A (172.20.120.12)
  [282:root]SSL state:SSLv3 write finished B (172.20.120.12)
  [282:root]SSL state:SSLv3 flush data (172.20.120.12)
  [282:root]SSL state:SSLv3 read finished A:system lib(172.20.120.12)
  [282:root]SSL state:SSLv3 read finished A (172.20.120.12)
  [282:root]SSL state:SSL negotiation finished successfully (172.20.120.12)
  [282:root]SSL established: DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
  ```

- Enter the following to stop displaying debug messages:

  ```
  diagnose debug disable
  ```

The following is a list of potential issues. The suggestions below are not exhaustive, and may not reflect your network topology.

There is no response from the SSL VPN URL.

- Go to **VPN > SSL > Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.
- Check the URL you are attempting to connect to. It should follow this pattern:

```
https://<FortiGate IP>:<Port>/remote/login
```

- Ensure that you are using the correct port number in the URL.

FortiClient cannot connect.

Read the Release Notes to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

Tunnel-mode connection shuts down after a few seconds.

This issue can occur when there are multiple interfaces connected to the Internet (for example, a dual WAN). Upgrade to the latest firmware then use the following CLI command:

```
config vpn ssl settings
   set route-source-interface enable
end
```

When you attempt to connect using FortiClient or in Web mode, you are returned to the login page, or you receive the following error message: "*Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12).*"

- Ensure that cookies are enabled in your browser.
- If you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.
- Access to the web portal or tunnel will fail if Internet Explorer has the privacy Internet Options set to High. If set to High, Internet Explorer will block cookies that do not have a compact privacy policy, and that use personally identifiable information without your explicit consent.

You receive an error message stating: "*Destination address of Split Tunneling policy is invalid.*"

The SSL VPN security policy uses the **ALL** address as its destination. Change the address to that of the protected network instead.

The tunnel connects but there is no communication.

Go to **Router > Static > Static Routes** and ensure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Go to **Policy & Objects > Policy > IPv4** and examine the policy allowing VPN access to the local network. If the destination address is set to all, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

Users are unable to download the SSL VPN plugin.

Go to **VPN > SSL > Portals** to make sure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

Users are being assigned to the wrong IP range.

Ensure that the same IP Pool is used in VPN Portal and VPN Settings to avoid conflicts. If there is a conflict, the portal settings will be used.

Sending tunnel statistics to FortiAnalyzer

By default, logged events include tunnel-up and tunnel-down status events. Other events, by default, will appear in the FortiAnalyzer report as "No Data Available". More accurate results require logs with `action=tunnel-stats`, which is used in generating reports on the FortiAnalyzer (rather than the tunnel-up and tunnel-down event logs). The FortiGate does not, by default, send `tunnel-stats` information.

To allow VPN `tunnel-stats` to be sent to FortiAnalyzer, configure the FortiGate unit as follows using the CLI:

```
config system settings
   set vpn-stats-log ipsec ssl
   set vpn-stats-period 300
end
```

Chapter 23 - System Administration

This guide contains the following sections:

Using the CLI provides an overview of the command line interface (CLI) for FortiOS. If you are new to the FortiOS CLI, this chapter provides a high level overview of how to use this method of administration.

Interfaces describes the FortiGate interface options and configuration choices.

Central management describes how to configure the FortiGate unit to use FortiManager as a method of maintaining the device and other features that FortiManager has to facilitate the administration of multiple devices.

Monitoring describes various methods of collecting log data and tracking traffic flows and tends.

VLANs discusses the implementation of virtual local area networks (VLANs) in FortiOS and how to configure and use them.

PPTP and L2TP describes these virtual private network (VPN) types and how to configure them.

Session helpers describes what session helpers are and how to view and configure them.

Advanced concepts describes more involved administrative topics to enhance network security and traffic efficiency.

Using the CLI

The command line interface (CLI) is an alternative configuration tool to the web-based manager. While the configuration of the web-based manager uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.

This section also explains common CLI tasks that an administrator does on a regular basis and includes the topics:

- Connecting to the CLI
- Command syntax
- Sub-commands
- Permissions
- Tips

Connecting to the CLI

You can access the CLI in three ways:

- Locally with a console cable — Connect your computer directly to the FortiGate unit's console port. Local access is required in some cases:
  - If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection.
  - Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until after the boot process has completed, making local CLI access the only viable option.
- Through the network — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect using the ***CLI Console*** widget in the web-based manager.
- Locally with FortiExplorer — Connect your computer directly to the FortiGate unit's USB management port. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port. To connect to the local console you need:

- A computer with an available serial communications (COM) port.
- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package.
- Terminal emulation software such as HyperTerminal for Microsoft Windows.

The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.

2. On your management computer, start HyperTerminal.
3. For the **Connection Description**, enter a **Name** for the connection, and select **OK**.
4. On the **Connect using** drop-down list box, select the communications (COM) port on your management computer you are using to connect to the FortiGate unit.
5. Select **OK**.
6. Select the following **Port** settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press **Enter** or **Return** on your keyboard to connect to the CLI.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

   The CLI displays the following text:

   ```
   Welcome!
   Type ? to list available commands.
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the **CLI Console** widget in the web-based manager.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is not connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer. You can do this using either a local console connection or the web-based manager.

Requirements

- A computer with an available serial communications (COM) port and RJ-45 port
- Terminal emulation software such as HyperTerminal for Microsoft Windows
- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
    end
```

   where:

   - `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
   - `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

   For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
config system interface
  edit port1
    set allowaccess ssh telnet
    end
```

5. To confirm the configuration, enter the command to display the network interface's settings.

```
show system interface <interface_str>
```

   The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1. On your management computer, start an SSH client.
2. In **Host Name (or IP Address)**, enter the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, enter `22`.
4. For the **Connection type**, select **SSH**.
5. Select **Open**.

   The SSH client connects to the FortiGate unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but used a different IP address or SSH key. This is normal If your management computer is directly connected to the FortiGate unit with no network hosts between them.

6. Click **Yes** to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.
7. The CLI displays a login prompt.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for this administrator account and press Enter.

   The FortiGate unit displays a command prompt (its host name followed by a `#`. You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept Telnet connections.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.

   The FortiGate unit displays a command prompt (its host name followed by a `#`. You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI locally with FortiExplorer

FortiExplorer is a standalone software solution that allows you to connect to your FortiGate device using the USB interface of your management computer. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

FortiExplorer is available for download from the Customer Service & Support website https://support.fortinet.com in firmware images. FortiExplorer is available for both Microsoft Windows and Mac OS X computers.

FortiExplorer provides a user-friendly tool that you can use to configure a FortiGate unit over a standard USB connection, rather than using a console cable or Ethernet connection.

Do not connect the USB cable until after FortiExplorer has been installed.

Installing FortiExplorer on Microsoft Windows

To install FortiExplorer on a Microsoft Windows workstation:

1. Double-click the .msi or .exe file and follow the instructions on-screen.
2. Connect the USB cable to the FortiGate unit and then to the management computer.
3. The FortiExplorer Fortinet Device Easy Configuration Utility opens when the USB cable is connected. Select ***Install the hardware automatically*** and select ***Next***.
4. After a moment, FortiExplorer will launch.

Installing FortiExplorer on Mac OS X

To install FortiExplorer on a Mac OS X workstation:

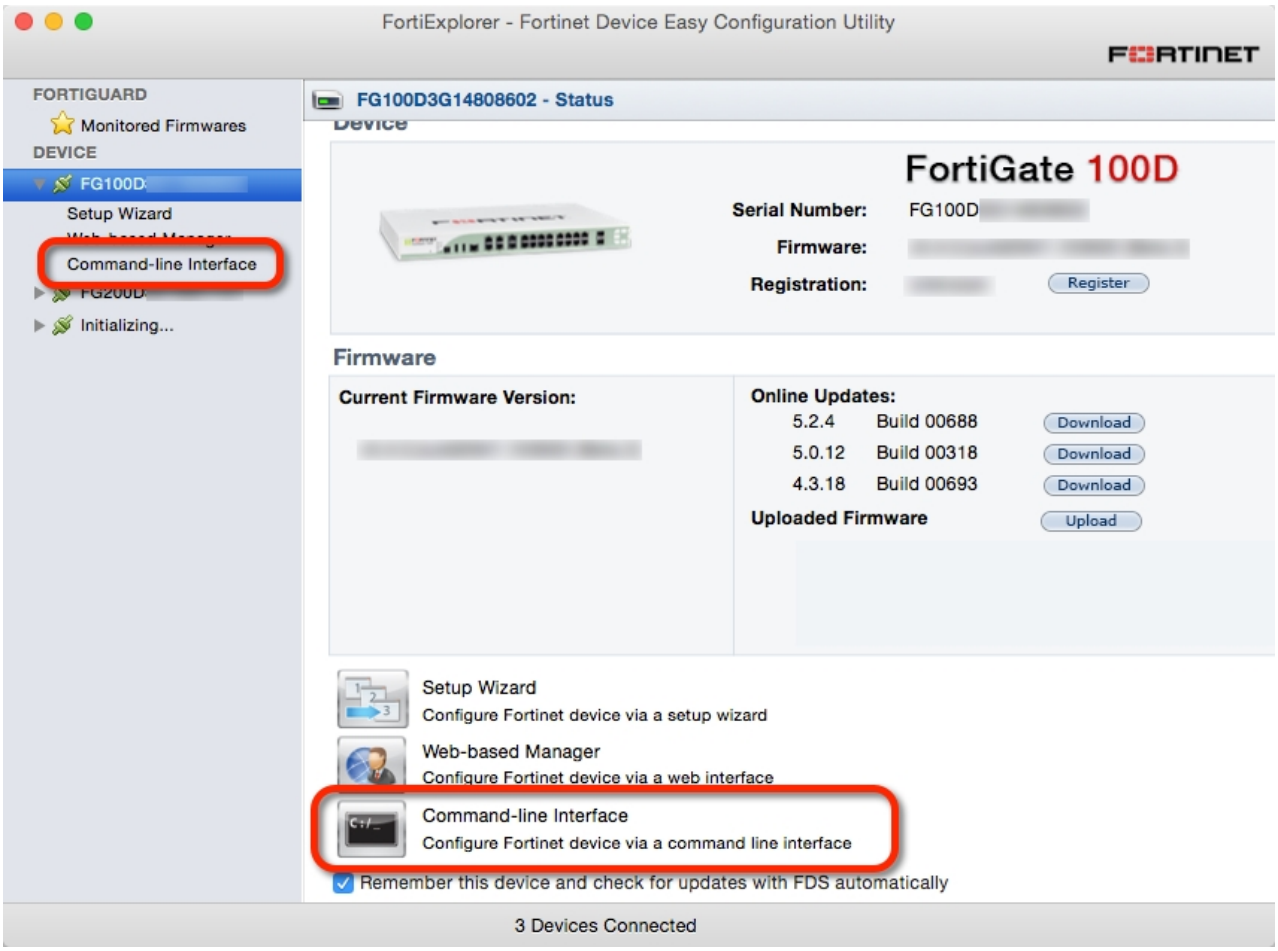
1. Double-click the .dmg file and drag the FortiExplorer program file into the Applications folder.
2. Connect the USB cable to the FortiGate unit and then to the management computer.
3. Double-click the FortiExplorer icon to launch the application.

Starting the CLI from FortiExplorer

The below image shows the FortiExplorer tool connected to a FortiGate 100D device. You have two options for connecting to the CLI.

1. The left window pan, in the ***Devices*** section, under the specific FortiGate's name, select on ***Command-line Interface.*** Select the text
2. In the main window pane, at the bottom, there is an icon of a terminal window beside the text ***Command-line Interface***. Select the icon.

Selecting either of these links will open a terminal emulation or command line interface in the main window pane of the FortiExplorer window.



Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the following conventions to describe valid command syntax

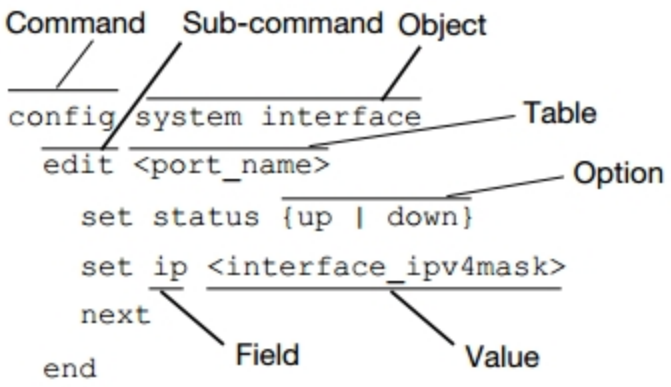
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multiline command lines, which can be entered using an escape sequence.
  Valid command lines must be unambiguous if abbreviated. Optional words or other command line permutations are indicated by syntax notation.
- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands.
  Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope.
- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them.
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation.
- **option** — A kind of value that must be one or more words from of a fixed set of options.

Indentation

Indentation indicates levels of nested commands, which indicate what other subcommittees are available from within the scope. For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      end
```

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention	Description
Square brackets `[ ]`	A non-required word or series of words. For example: `[verbose {1 | 2 | 3}]` indicates that you may either omit or type both the `verbose` word and its accompanying option, such as `verbose 3`.
Angle brackets `< >`	A word constrained by data type. The angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example, `<retries_int>`, indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@example.com`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.168.1.1/24` • `<xxx_ipv4range>` : A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. • `<xxx_str>`: A string of characters that is not another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. • `<xxx_int>`: An integer number that is **not** another data type, such as `15` for the number of minutes.

Convention	Description
Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets `[ ]`.
Options delimited by vertical bars `|`	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`

Sub-commands

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands.When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      next
   end
```

Sub-command scope is indicated by indentation.

Available sub-commands vary by command. From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Commands for tables

clone <table>	Clone (or make a copy of) a table from the current object.
	
	For example, in `config firewall policy`, you could enter the following command to clone security policy 27 to create security policy 30:
	
	`clone 27 to 30`
	
	In `config antivirus profile`, you could enter the following command to clone an antivirus profile named `av_pro_1` to create a new antivirus profile named `av_pro_2`:
	
	`clone av_pro_1 to av_pro_2`
	
	`clone` may not be available for all tables.

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables. In objects such as security policies, `<table>` is a sequence number. To create a new entry without the risk of overwriting an existing one, enter `edit 0`. The CLI initially confirms the creation of entry 0, but assigns the next unused number after you finish editing and enter `end`.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.

get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see the CLI Reference.
purge	Remove all tables in the current object. For example, in `config user local`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiGate unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.
rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
append	Add an option to an existing list.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
move	Move an object within a list, when list order is important. For example, rearranging security policies within the policy list.
next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set password newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unselect	Remove an option from an existing list.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset password` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Depending on the account that you use to log in to the FortiGate unit, you may not have complete access to all CLI commands. Access profiles control which CLI commands an administrator account can access. Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access.

Unlike other administrator accounts, the administrator account named `admin` exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing **all** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

Set a strong password for the admin administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the admin administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

Adding and removing options from lists

When adding options to a list, such as a user group, using the `set` command will remove the previous configuration. For example. if you wish to add user D to a user group that already contains members A, B, and C, the command would need to be `set member A B C D`. If only `set member D` was used, then all former members would be removed from the group.

However, there are additional commands which can be used instead of `set` for changing options in a list.

Additional commands for lists

append	Add an option to an existing list. For example, `append member` would add user D to a user group while all previous group members are retained
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.
unselect	Remove an option from an existing list. For example, `unselect member A` would remove member A from a group will all previous group members are retained.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

Environment variables

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the **CLI Console** widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
   set hostname $SerialNum
end
```

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields. These characters are special characters, also known as reserved characters.

You may be able to enter special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\ ) character.

In other cases, different keystrokes are required to input a special character. If you need to enter ? as part of config, you first need to input CTRL-V. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: `"Security Administrator"`. Enclose the string in single quotes: `'Security Administrator'`. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Using grep to filter get and show command output

In many cases, the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large get or show command output, you can use the grep command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX grep, used for searching text output based on regular expressions.

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr             00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
```

Use the following command to display all lines in HTTP replacement message commands that contain `URL` (upper or lower case):

```
show system replacemsg http | grep -i url
```

There are three additional options that can be applied to grep:

```
-A <num> After
-B <num> Before
-C <num> Context
```

The option `-f` is also available to support Fortinet contextual output, in order to show the complete configuration. The following example shows the difference in output when `-f` option is used versus when it is not.

Using -f:

```
show | grep -f ldap-group1
   config user group
      edit "ldap-group1"
         set member "pc40-LDAP"
      next
   end
   config firewall policy
      edit 2
         set srcintf "port31"
         set dstintf "port32"
         set srcaddr "all"
         set action accept
         set identity-based enable
         set nat enable
         config identity-based-policy
            edit 1
               set schedule "always"
               set groups "ldap-group1"
               set dstaddr "all"
               set service "ALL"
            next
         end
      next
   end
```

Without using -f:

```
show | grep ldap-group1
   edit "ldap-group1"
      set groups "ldap-group1"
```

Language support and regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice. To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\ ) could be inadvertently interpreted as the symbol for the Japanese yen (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work it if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.

HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

If you configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

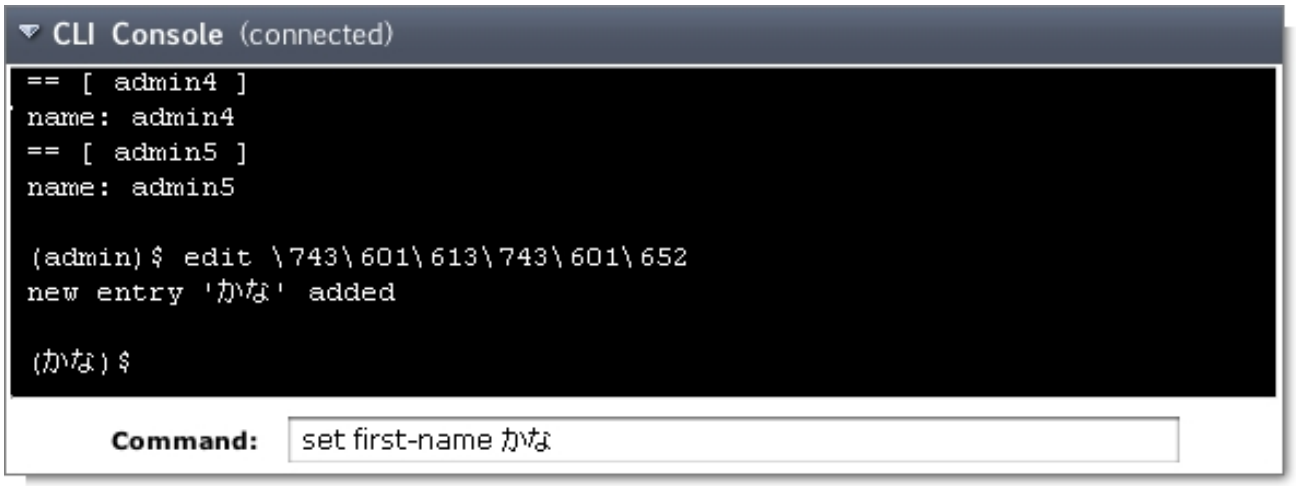
Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web-based manager or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

To enter non-ASCII characters in the CLI Console widget

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's web-based manager.

2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Go to **System > Dashboard > Status**.
5. In title bar of the **CLI Console** widget, click **Edit** (the pencil icon).
6. Enable **Use external command input box**.
7. Select **OK**.
8. The **Command** field appears below the usual input and display area of the **CLI Console** widget.
9. In **Command**, type a command.

Entering encoded characters (CLI Console widget):



10. Press **Enter**.
    In the display area, the ***CLI Console*** widget displays your previous command interpreted into its character code equivalent, such as:

    ```
    edit \743\601\613\743\601\652
    ```

    and the command's output.

To enter non-ASCII characters in a Telnet/SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.
   Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press Enter.

Entering encoded characters (PuTTY):

You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

Screen paging

You can configure the CLI to pause after displaying each page's worth of text when displaying multiple pages of output. When the display pauses, the last line displays `--More--`. You can then either:

- press the spacebar to display the next page.
- type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
   set output more
end
```

Baud rate

You can change the default baud rate of the local console connection.

To change the baud rate enter the following commands:

```
config system console
   set baudrate {115200 | 19200 | 38400 | 57600 | 9600}
end
```

Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be timesaving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.

Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

3. Use `execute restore` to upload the modified configuration file back to the FortiGate unit.
   The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the FortiGate unit restarts and loads the new configuration.

Using Perl regular expressions

Some FortiGate features, such as spam filtering and web content filtering can use either wildcards or Perl regular expressions.

See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions. For more information on using Perl expressions see the Security Profiles chapter of The Handbook.

Differences between regular expression and wildcard pattern matching

In Perl regular expressions, the period (‘.’) character refers to any single character. It is similar to the question mark (‘?’) character in wildcard pattern matching. As a result:

- `fortinet.com` not only matches `example.com` but also matches `exampleacom`, `examplebcom`, `exampleccom` and so on.

To match a special character such as the period ('.') and the asterisk (‘*’), regular expressions use the slash (‘\’) escape character. For example:

- To match `example.com`, the regular expression should be `example\.com`.

In Perl regular expressions, the asterisk (‘*’) means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- `exam*\.com` matches `exammmm.com` but does not match `eample.com`.

To match any character 0 or more times, use ‘.*’ where ‘.’ means any character and the ‘*’ means 0 or more times. For example:

- the wildcard match pattern `exam*.com` is equivalent to the regular expression `exam.*\.com`.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression “test” not only matches the word “test” but also matches any word that contains the word “test” such as

“atest”, “mytest”, “testimony”, “atestb”. The notation “\b” specifies the word boundary. To match exactly the word “test”, the expression should be `\btest\b`.

Case sensitivity

Regular expression pattern matching is case sensitive in the Web and Spam filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of “bad language” regardless of case.

Perl regular expression examples

Expression	Matches
abc	abc (that exact character sequence, but anywhere in the string)
^abc	abc at the beginning of the string
abc$	abc at the end of the string
a|b	either of a and b
^abc|abc$	the string abc at the beginning or at the end of the string
ab{2,4}c	an a followed by two, three or four b's followed by a c
ab{2,}c	an a followed by at least two b's followed by a c
ab*c	an a followed by any number (zero or more) of b's followed by a c
ab+c	an a followed by one or more b's followed by a c
ab?c	an a followed by an optional b followed by a c; that is, either abc or ac
a.c	an a followed by any single character (not newline) followed by a c
a\.c	a.c exactly
[abc]	any one of a, b and c
[Aa]bc	either of Abc and abc
[abc]+	any (nonempty) string of a's, b's and c's (such as a, abba, acbabcacaa)
[^abc]+	any (nonempty) string which does not contain any of a, b and c (such as defg)
\d\d	any two decimal digits, such as 42; same as \d{2}
/i	makes the pattern case insensitive. For example, `/bad language/i` blocks any instance of “bad language” regardless of case.
\w+	a "word": a nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	the strings 100 and mk optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	abc when followed by a word boundary (e.g. in abc! but not in abcd)
perl\B	perl when not followed by a word boundary (e.g. in perlert but not in perl stuff)

Expression	Matches
\x	tells the regular expression parser to ignore white space that is neither backslashed nor within a character class. You can use this to break up your regular expression into (slightly) more readable parts.

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the Release Notes for a new firmware release.
- Review the Supported Upgrade Paths document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration, including local certificates. For more information, see Firmware on page 2243.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Backing up the current configuration

In case you need to restore your FortiGate configuration, you should always back up the configuration before installing new firmware.

To create a local backup:

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Select **Backup** beside **System Configuration**.
3. Choose either **Local PC** or **USB Disk** to save the configuration file.
4. If desired, select **Encrypt configuration file**.
5. Select **Backup**.

Restoring a configuration file

Rather than reconfigure the FortiGate manually, it is possible to upload a saved configuration file.

To restore your FortiGate configuration

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Select **[Restore]** beside **System Configuration**.
3. Choose either **Local PC** or **USB Disk** depending the location of the file.
4. Select ***Choose File*** and browse to the correct file in the file manager window.

5. If a password was associated with the configuration file, enter it in the ***Password*** field.
6. Select **Restore**.

Troubleshooting

During the installation there are some possible errors that you may come across but the solutions are usually straightforward.

.

Error message	Reason and Solution
Configuration file error	This error occurs when attempting to upload a configuration file that is incompatible with the device. This may be due to the configuration file being for a different model or being saved from a different version of firmware. **Solution**: upload a configuration file that is for the correct model of FortiGate device and the correct version of the firmware.
Invalid password	When the configuration file is saved, it can be protected by a password. The password entered during the upload process is not matching the one associated with the configuration file. **Solution**: use the correct password if the file is password protected.

Downloading firmware

Firmware images for all FortiGate units is available on the Fortinet Customer Support website, https://support.fortinet.com.

To download firmware

1. Log into the site using your user name and password.
2. Go to **Download > Firmware Images**.
3. A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware you wish to upgrade your FortiGate unit to.
4. Select **HTTPS Download**.

Firmware can also be downloaded using FTP; however, as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

5. Navigate to find the folder for the firmware version you wish to use.
6. Select your FortiGate model from the list. If your unit is a FortiWiFi, be sure to get the appropriate firmware, which will have a filename starting with FWF.
7. Save the firmware image to your computer.

Testing new firmware

The integrity of a firmware images downloaded from Fortinet's support portal can be verified using a file checksum. A file checksum that does not match the expected value indicates a corrupt file. The corruption could be caused by errors in transfer or by file modification. A list of expected checksum values for each build of released code is available on Fortinet's support portal.

Image integrity is also verified when the FortiGate is booting up. This integrity check is done through cyclic redundancy check (CRC). If the CRC fails, the Fortinet unit will error during the boot process, preventing suboptimal operation of the device.

Lastly, firmware images are signed and the signature is attached to the code as it is built. When upgrading an image, the running OS will generate a signature and compare it with the signature attached to the image. If the signatures do not match, the new OS will not load.

Testing before installation

FortiOS enables you to test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure Testing new firmware on page 2245 .

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 or null modem cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure, you must install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Enter the following command to restart the FortiGate unit:
   ```
   execute reboot
   ```
6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages appears.
   When the following messages appears:
   ```
   Press any key to display configuration menu....
   ```
7. Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must login and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
    [H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press **Enter**.

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address of the FortiGate unit to connect to the TFTP server.

    The IP address must be on the same network as the TFTP server.

Make sure you do not enter the IP address of another device on this network.

    The following message appears:

    ```
    Enter File Name [image.out]:
    ```

11. Enter the firmware image file name and press **Enter**.

    The TFTP server uploads the firmware image file to the FortiGate unit and the following appears.

    ```
    Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
    ```

12. Type `R`.

    The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

You can test the new firmware image as required. When done testing, you can reboot the FortiGate unit, and the FortiGate unit will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware - web-based manager

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware

1. Log into the web-based manager as the admin administrative user.
2. Go to **System > Dashboard > Status** and locate the **System Information** widget.
3. Beside **Firmware Version**, select **Update**.
4. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
5. Select **OK**.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

Upgrading the firmware - CLI

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For more information, see the System Administration handbook.

Before you begin, ensure you have a TFTP server running and accessible to the FortiGate unit.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware using the CLI

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The FortiGate unit responds with the message:

   ```
   This operation will replace the current firmware version!
       Do you want to continue? (y/n)
   ```

6. Type `y`.
7. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

8. Reconnect to the CLI.
9. Update antivirus and attack definitions, by entering:

```
execute update-now
```

Installing firmware from a system reboot using the CLI

There is a possibility that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots. If this occurs, it is best to perform a fresh install of the firmware from a reboot using the CLI.

This procedure installs a firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9, or null modem cable. This procedure reverts the FortiGate unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the FortiGate unit configuration.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

6. Enter the following command to restart the FortiGate unit.

```
execute reboot
```

   The FortiGate unit responds with the following message:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

7. Type `y`.

   As the FortiGate unit starts, a series of system startup messages appears. When the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get to the new firmware image form the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press **Enter**.

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image filename and press **Enter**.

    The TFTP server uploads the firmware image file to the FortiGate unit and a message similar to the following appears:

    ```
    Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
    ```

12. Type `D`.

    The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Reverting to a previous firmware version - web-based manager

The following procedures revert the FortiGate unit to its factory default configuration and deletes any configuration settings. If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Always remember to back up your configuration before making any changes to the firmware.

To revert to a previous firmware version

1. Go to **System > Dashboard > Status** and locate the **System Information widget**.
2. Beside **Firmware Version**, select **Update**.
3. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
4. Select **OK**.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

Reverting to a previous firmware version - CLI

This procedure reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

To use the following procedure, you must have a TFTP server the FortiGate unit can connect to.

To revert to a previous firmware version using the CLI

1. Make sure the TFTP server is running
2. Copy the firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI.
4. Make sure the FortiGate unit can connect to the TFTP server execute by using the `execute ping` command.
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image28.out 192.168.1.168
   ```

   The FortiGate unit responds with this message:

   ```
   This operation will replace the current firmware version!
       Do you want to continue? (y/n)
   ```

6. Type `y`.

   The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

   ```
   Get image from tftp server OK.
   ```

```
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7. Type `y`.
8. The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
9. Reconnect to the CLI.
10. To restore your previous configuration, if needed, use the command:
```
execute restore config <name_str> <tftp_ip4>
```
11. Update antivirus and attack definitions using the command:
```
execute update-now.
```

Configuration revision

The **Configuration Revisions** menu enables you to manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive. The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed in the **System Information** widget on the Dashboard.

Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can also be configured so that when it is rebooted, it will automatically load the new firmware (CLI only). Using this option, you can stage a number of FortiGate units to do an upgrade simultaneously to all devices using FortiManager or script.

To load the firmware for later installation - web-based manager

1. Go to **System > Dashboard > Status**.
2. Under **System Information > Firmware Version**, select **Update**.
3. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
4. Deselect the **Boot the New Firmware** option.
5. Select **OK**.

To load the firmware for later installation - CLI

```
execute restore secondary-image {ftp | tftp | usb}
```

To set the FortiGate unit so that when it reboots, the new firmware is loaded, use the CLI command…

```
execute set-next-reboot {primary | secondary}
```

... where `{primary | secondary}` is the partition with the preloaded firmware.

To trigger the upgrade using the web-based manager

1. Go to **System > Dashboard > Status**.
2. Under **System Information > Firmware Version**, select **Details**.
3. Select the check box for the new firmware version.
   The **Comments** column indicates which firmware version is the current active version.
4. Select **Upgrade** icon.

Interfaces

Interfaces, both physical and virtual, enable traffic to flow to and from the internal network, and the Internet and between internal networks. The FortiGate unit has a number of options for setting up interfaces and groupings of subnetworks that can scale to a company's growing requirements.

This chapter includes:

- Physical
- Interface settings
- Software switch
- Virtual Switch
- Loopback interfaces
- Redundant interfaces
- One-armed sniffer
- Aggregate Interfaces
- DHCP addressing mode on an interface
- Administrative access
- Wireless
- Interface MTU packet size
- Secondary IP addresses to an interface
- Virtual domains
- Virtual LANs
- Zones

Physical

FortiGate units have a number of physical ports where you connect ethernet or optical cables. Depending on the model, they can have anywhere from four to 40 physical ports. Some units have a grouping of ports labelled as internal, providing a built-in switch functionality.

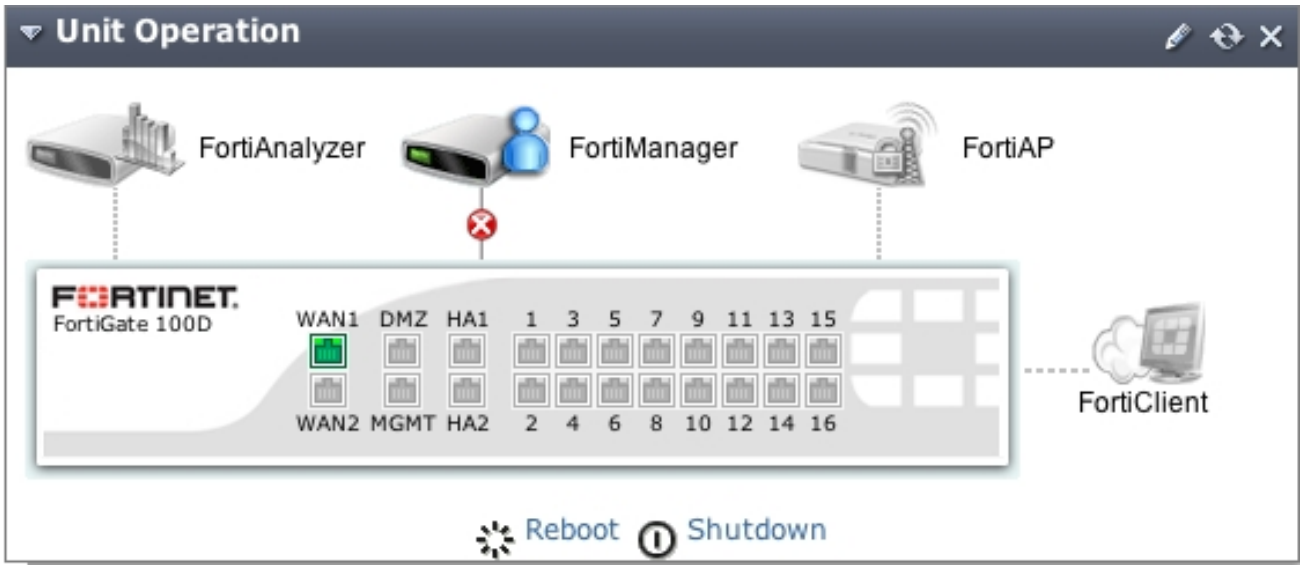
In FortiOS, the port names, as labeled on the FortiGate unit, appear in the web-based manager in the **Unit Operation** widget, found on the Dashboard. They also appear when you are configuring the interfaces, by going to **System > Network > Interface**. As shown below, the FortiGate-100D (Generation 2) has 22 interfaces.

Two of the physical ports on the FortiGate-100D (Generation 2) are SFP ports. These ports share the numbers 15 and 16 with RJ-45 ports. Because of this, when SFP port 15 is used, RJ-45 port 15 cannot be used, and vice versa.

These ports also share the same MAC address.

FortiGate-100D physical interfaces

FortiGate-100D interfaces on the Dashboard



Configuring the FortiGate-100D ports

	Name	Type	IP/Netmask	Access	Administrative Status	Link Status	Ref.
☐	wan1	Physical	172.20.120.230 / 255.255.255.0	HTTP,HTTPS,PING,SSH	↑	↑ 100 Mbps/Full Duplex	1
☐	dmz	Physical	10.10.10.1 / 255.255.255.0	HTTPS,PING,FMG-Access	↑	↓	1
☐	modem	Physical	0.0.0.0 / 0.0.0.0		↓	↓	0
☐	wan2	Physical	0.0.0.0 / 0.0.0.0	PING,FMG-Access	↑	↓	1
☐	mgmt	Physical	192.168.1.99 / 255.255.255.0	HTTPS,PING,FMG-Access	↑	↓	0
☐	ha1	Physical	0.0.0.0 / 0.0.0.0		↑	↓	0
☐	ha2	Physical	0.0.0.0 / 0.0.0.0		↑	↓	0
☐	internal	Physical	192.168.100.99 / 255.255.255.0	HTTPS,PING,FMG-Access	↑	↑ 100 Mbps/Full Duplex	3

Normally the internal interface is configured as a single interface shared by all physical interface connections - a switch. The switch mode feature has two states - switch mode and interface mode. Switch mode is the default mode with only one interface and one address for the entire internal switch. Interface mode enables you to configure each of the internal switch physical interface connections separately. This enables you to assign different subnets and netmasks to each of the internal physical interface connections.

The larger FortiGate units can also include Advanced Mezzanine Cards (AMC), which can provide additional interfaces (Ethernet or optical), with throughput enhancements for more efficient handling of specialized traffic. These interfaces appear in FortiOS as port amc/sw1, amc/sw2 and so on. In the following illustration, the FortiGate-3810A has three AMC cards installed: two single-width (amc/sw1, amc/sw2) and one double-width (amc/dw).

FortiGate-3810A AMC card port naming

	Name	IP/Netmask	Access	Administrative Status	Link Status
☐	amc-dw2/1	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-dw2/2	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw1/1	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw1/2	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw1/3	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw1/4	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw2/1	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw2/2	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw2/3	0.0.0.0 / 0.0.0.0		↑	↓
☐	amc-sw2/4	0.0.0.0 / 0.0.0.0		↑	↓
☐	april	0.0.0.0 / 0.0.0.0		↑	
☐	port1	10.21.101.101 / 255.255.255.0	HTTPS,PING,SSH	↑	↑
☐	port2	192.168.100.99 / 255.255.255.0	PING	↑	↓
☐	port3	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port4	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port5	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port6	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port7	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port8	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port9	0.0.0.0 / 0.0.0.0	PING	↑	↓
☐	port10	0.0.0.0 / 0.0.0.0	PING	↑	↓

Interface settings

In **System > Network > Interface**, you configure the interfaces, physical and virtual, for the FortiGate unit. There are different options for configuring interfaces when the FortiGate unit is in NAT mode or transparent mode. On FortiOS Carrier, you can also enable the Gi gatekeeper on each interface for anti-overbilling.

Interface page	
Create New	Select to add a new interface, zone or, in transparent mode, port pair. For more information on configuring zones, see Zones. Depending on the model you can add a VLAN interface, a loopback interface, a IEEE 802.3ad aggregated interface, or a redundant interface. When VDOMs are enabled, you can also add Inter-VDOM links.
Name	The names of the physical interfaces on your FortiGate unit. This includes any alias names that have been configured. When you combine several interfaces into an aggregate or redundant interface, only the aggregate or redundant interface is listed, not the component interfaces. If you have added VLAN interfaces, they also appear in the name list, below the physical or aggregated interface to which they have been added. If you have added loopback interfaces, they also appear in the interface list, below the physical interface to which they have been added. If you have software switch interfaces configured, you will be able to view them. If your FortiGate unit supports AMC modules, the interfaces are named amc-sw1/1, amc-dw1/2, and so on.
Type	The configuration type for the interface.
IP/Netmask	The current IP address and netmask of the interface. In VDOM, when VDOMs are not all in NAT or transparent mode some values may not be available for display and will be displayed as “-”.
Access	The administrative access configuration for the interface.
Administrative Status	Indicates if the interface can be accessed for administrative purposes. If the administrative status is a green arrow, and administrator could connect to the interface using the configured access. If the administrative status is a red arrow, the interface is administratively down and cannot be accessed for administrative purposes.
Link Status	The status of the interface physical connection. Link status can be either up (green arrow) or down (red arrow). If link status is up the interface is connected to the network and accepting traffic. If link status is down the interface is not connected to the network or there is a problem with the connection. You cannot change link status from the web-based manager, and typically is indicative of an ethernet cable plugged into the interface. Link status is only displayed for physical interfaces.

Interface page	
MAC	The MAC address of the interface.
Mode	Shows the addressing mode of the interface. The addressing mode can be manual, DHCP, or PPPoE.
Secondary IP	Displays the secondary IP addresses added to the interface.
MTU	The maximum number of bytes per transmission unit (MTU) for the interface.
Virtual Domain	The virtual domain to which the interface belongs. This column is visible when VDOM configuration is enabled.
VLAN ID	The configured VLAN ID for VLAN subinterfaces.

Interface configuration and settings

To configure an interface, go to **System > Network > Interface and** select **Create New**.

Name	Enter a name of the interface. Physical interface names cannot be changed.
Alias	Enter an alternate name for a physical interface on the FortiGate unit. This field appears when editing an existing physical interface. The alias can be a maximum of 25 characters. The alias name will not appears in logs.
Link Status	Indicates whether the interface is connected to a network (link status is **Up**) or not (link status is **Down**). This field appears when editing an existing physical interface.
Type	Select the type of interface that you want to add. On some models you can set **Type** to **802.3ad Aggregate** or **Redundant Interface**.
Interface	Displayed when **Type** is set to **VLAN**. Select the name of the physical interface to which to add a VLAN interface. Once created, the VLAN interface is listed below its physical interface in the Interface list. You cannot change the physical interface of a VLAN interface except when adding a new VLAN interface.
VLAN ID	Displayed when **Type** is set to **VLAN**. Enter the VLAN ID. You cannot change the **VLAN ID** except when adding a new VLAN interface. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface.
Virtual Domain	Select the virtual domain to add the interface to. Admin accounts with super_admin profile can change the **Virtual Domain**.

Physical Interface Members	This section has two different forms depending on the interface type: • **Software switch interface** - this section is a display-only field showing the interfaces that belong to the software switch virtual interface. • **802.3ad aggregate or Redundant interface** - this section includes available interface and selected interface lists to enable adding or removing interfaces from the interface. Select interfaces from this **Available Interfaces** list and select the right arrow to add an interface to the **Selected Interface** list.
Addressing mode	Select the addressing mode for the interface. • Select **Manual** and add an **IP/Netmask** for the interface. If IPv6 configuration is enabled you can add both a IPv4 and an IPv6 IP address. • Select **DHCP** to get the interface IP address and other network settings from a DHCP server. • Select **PPPoE** to get the interface IP address and other network settings from a PPPoE server. • Select **One-Arm Sniffer** to enable the interface as a means to detect possible traffic threats. This option is available on physical ports not configured for the primary Internet connection. • Select **Dedicate to FortiAP/FortiSwitch** to have a FortiAP unit or FortiSwitch unit connect exclusively to the interface. This option is only available when editing a physical interface, and it has a static IP address. When you enter the IP address, the FortiGate unit automatically creates a DHCP server using the subnet entered. This option is not available on the ADSL interface. The FortiSwitch option is currently only available on the FortiGate-100D.
IP/Netmask	If **Addressing Mode** is set to **Manual**, enter an IPv4 address/subnet mask for the interface. FortiGate interfaces cannot have IP addresses on the same subnet.
IPv6 Address	If **Addressing Mode** is set to **Manual** and IPv6 support is enabled, enter an IPv6 address/subnet mask for the interface. A single interface can have both an IPv4 and IPv6 address or just one or the other.
Administrative Access	Select the types of administrative access permitted for IPv4 connections to this interface.
HTTPS	Allow secure HTTPS connections to the web-based manager through this interface. If configured, this option will enable automatically when selecting the **HTTP** option.
PING	Interface responds to pings. Use this setting to verify your installation and for testing.

HTTP	Allow HTTP connections to the web-based manager through this interface. If configured, this option will also enable the **HTTPS** option.
SSH	Allow SSH connections to the CLI through this interface.
SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
TELNET	Allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.
FMG-Access	Allow FortiManager authorization automatically during the communication exchange between the FortiManager and FortiGate units.
FCT-Access	You can configure a FortiGate interface as an interface that will accept FortiClient connections. When configured, the FortiGate unit sends broadcast messages which the FortiClient software running on a end user PC is listening for.
CAPWAP	Allows the FortiGate unit's wireless controller to manage a wireless access point, such as a FortiAP unit.
IPv6 Administrative Access	Select the types of administrative access permitted for IPv6 connections to this interface. These types are the same as for Administrative Access.
Security Mode	Select a captive portal for the interface. When selected, you can define the portal message and look that the user sees when logging into the interface. You can also define one or more user groups that have access to the interface.
DHCP Server	Select to enable a DHCP server for the interface. For more information on configuring a DHCP server on the interface, see DHCP servers and relays.
Detect and Identify Devices	Select to enable the interface to be used with BYOD hardware such as iPhones. Define the device definitions by going to **User & Device > Device**.
Add New Devices to Vulnerability Scan List	This option appears when **Detect and Identify Devices** is enabled. When enabled, the FortiGate unit performs a network vulnerability scan of any devices detected or seen on the interface. The vulnerability scan occur as configured, either on demand, or as scheduled.

Broadcast Discovery Messages	Available when **FCT-Access** is enabled for the **Administrative Access**. Select to enable sends broadcast messages which the FortiClient software running on a end user PC is listening for. Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message.
Enable Explicit Web Proxy	Available when enabling explicit proxy on the **System Information** Dashboard (**System > Dashboard > Status**). This option is not available for a VLAN interface selection. Select to enable explicit web proxying on this interface. When enabled, this interface will be displayed on **System > Network > Explicit Proxy** under **Listen on Interfaces** and web traffic on this interface will be proxied according to the Web Proxy settings.
Enable STP	With FortiGate units with a switch interface is in switch mode, this option is enabled by default. It enables the single instance MSTP spanning tree protocol.
Listen for RADIUS Accounting Messages	Select to use the interface as a listening port for RADIUS content.
Secondary IP Address	Add additional IPv4 addresses to this interface. Select the Expand Arrow to expand or hide the section.
Comments	Enter a description up to 255 characters to describe the interface.
Administrative Status	Select either **Up** (green arrow) or **Down** (red arrow) as the status of this interface. **Up** indicates the interface is active and can accept network traffic. **Down** indicates the interface is not active and cannot accept traffic.
Gi Gatekeeper (FortiOS Carrier only)	For FortiOS Carrier, enable Gi Gatekeeper to enable the Gi firewall as part of the anti-overbilling configuration. You must also configure **Gi Gatekeeper Settings** by going to **System > Admin > Settings**.

Software switch

A software switch, or soft switch, is a virtual switch that is implemented at the software, or firmware level, rather than the hardware level. A software switch can be used to simplify communication between devices connected to different FortiGate interfaces. For example, using a software switch, you can place the FortiGate interface connected to an internal network on the same subnet as your wireless interfaces. Then devices on the internal network can communicate with devices on the wireless network without any additional configuration such as additional security policies, on the FortiGate unit.

It can also be useful if you require more hardware ports on for the switch on a FortiGate unit. For example, if your FortiGate unit has a 4-port switch, WAN1, WAN2 and DMZ interfaces, and you need one more port, you can create a soft switch that can include the 4-port switch and the DMZ interface all on the same subnet. These types of applications also apply to wireless interfaces and virtual wireless interfaces and physical interfaces such as those with FortiWiFi and FortiAP unit.

Similar to a hardware switch, a software switch functions like a single interface. A software switch has one IP address; all of the interfaces in the software switch are on the same subnet. Traffic between devices connected to each interface are not regulated by security policies, and traffic passing in and out of the switch are affected by the same policy.

There are a few things to consider when setting up a software switch:

- Ensure you create a back up of the configuration.
- Ensure you have at least one port or connection such as the console port to connect to the FortiGate unit. If you accidentally combine too many ports, you will need a way to undo any errors.
- The ports that you include must not have any link or relation to any other aspect of the FortiGate unit. For example, DHCP servers, security policies, and so on.
- For increased security, you can create a captive portal for the switch, allowing only specific user groups access to the resources connected to the switch.

To create a software switch - web-based manager

1. Go to **System > Network > Interface** and select **Create New**.
2. For **Type**, select **Software Switch**.
3. In the **Physical Interface Members** option, select the interfaces to include.
4. Configure the remaining interface settings
5. Select **OK**.

To create a software switch - CLI

```
config system switch-interface
   edit <switch-name>
      set type switch
      set member <interface_list>
end
config system interface
   edit <switch_name>
      set ip <ip_address>
      set allowaccess https ssh ping
end
```

Soft switch example

For this example, the wireless interface (WiFi) needs to be on the same subnet as the DMZ1 interface to facilitate wireless syncing from an iPhone and a local computer. The synching between two subnets is problematic. By putting both interfaces on the same subnet the synching will work. The software switch will accomplish this.

In this example, the soft switch includes a wireless interface. Remember to configure any wireless security before proceeding. If you leave this interface open without any password or other security, it leaves open access to not only the wireless interface but to any other interfaces and devices connected within the software switch.

Clear the interfaces and back up the configuration

First, ensure that the interfaces are not being used with any other security policy or other use on the FortiGate unit. Check the WiFi and DMZ1 ports to ensure DHCP is not enabled on the interface and there are no other dependencies with these interfaces.

Next, save the current configuration, in the event something doesn't work, recovery can be quick.

Merge the interfaces

The plan is to merge the WiFi port and DMZ1 port. This will create a software switch with a name of "synchro" with an IP address of 10.10.21.12. The steps will create the switch, add the IP and then set the administrative access for HTTPS, SSH and Ping.

To merge the interfaces - CLI

```
config system switch-interface
   edit synchro
      set type switch
      set member dmz1 wifi
end
config system interface
   edit synchro
      set ip 10.10.21.12
      set allowaccess https ssh ping
end
```

Final steps

With the switch set up, you can now add security policies, DHCP servers an any other configuration that you would normally do to configure interfaces on the FortiGate unit.

Virtual Switch

Virtual switch feature enables you create virtual switches on top of the physical switch(es) with designated interfaces/ports so that a virtual switch can build up its forwarding table through learning and forward traffic accordingly. When traffic is forwarded among interfaces belonging to the same virtual switch, the traffic doesn't need to go up to the software stack, but forwarded directly by the switch. When traffic has to be relayed to interfaces not on the virtual switch, the traffic will go through the normal data path and be offloaded to NP4 when possible.

This feature is only available on mid to high end FortiGate units, including the 100D, 600C, 1000C, and 1240B.

To enable and configure the virtual switch, enter the CLI commands:

```
config system virtual-switch
   edit vs1
      set physical-switch sw0
         config port
            edit 1
               set port port1
               set speed xx
               set duplex xx
```

```
            set status [up|down]
        edit 2
            set port port2
            set ...
        end
    end
end
```

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The FortiGate's loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. Multiple loopback interfaces can be configured in either non-VDOM mode or in each VDOM.

Loopback interfaces still require appropriate firewall policies to allow traffic to and from this type of interface.

A loopback interface can be used with:

- Management access
- BGP (TCP) peering
- PIM RP

Loopback interfaces are a good practice for OSPF. Setting the OSPF router ID the same as loopback IP address troubleshooting OSPF easier, and remembering the management IP addresses (telnet to “router ID”).

Dynamic routing protocols can be enabled on loopback interfaces

For black hole static route, use the black hole route type instead of the loopback interface.

Redundant interfaces

On some models you can combine two or more physical interfaces to provide link redundancy. This feature enables you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for distribution of increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

An interface is available to be in a redundant interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of an aggregated or redundant interface
- it is in the same VDOM as the redundant interface
- it has no defined IP address
- is not configured for DHCP or PPPoE
- it has no DHCP server or relay configured on it
- it does not have any VLAN subinterfaces
- it is not referenced in any security policy, VIP, or multicast policy

- it is not monitored by HA
- it is not one of the FortiGate-5000 series backplane interfaces

When an interface is included in a redundant interface, it is not listed on the **System > Network > Interface** page. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, or routing.

One-armed sniffer

A one-armed sniffer is used to configure a physical interface on the FortiGate unit as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. Sniffing only reports on attacks. It does not deny or otherwise influence traffic.

Using the one-arm sniffer, you can configure a FortiGate unit to operate as an IDS appliance by sniffing network traffic for attacks without actually processing the packets. To configure one-arm IDS, you enable sniffer mode on a FortiGate interface and connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

To assign an interface as a sniffer interface, go to **System > Network > Interface**, edit the interface and select **One-Arm Sniffer**.

If the check box is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs or other features in which a physical interface is specified.

Enable Filters	Select to include filters to define a more granular sniff of network traffic. Select specific addresses, ports, VLANs and protocols. In all cases, enter a number, or number range, for the filtering type. For Protocol values, standard protocols are: • UDP - 17 • TCP - 6 • ICMP - 1
Include IPv6 Packets	If your network is running a combination of IPv4 and IPv6 addressing, select to sniff both addressing types. Otherwise, the FortiGate unit will only sniff IPv4 traffic.
Include Non-IP Packets	Select for a more intense scan of content in the traffic.
UTM Security Profiles	IPS sensors, and application control lists enable you to select specific sensors and application you want to identify within the traffic.

Aggregate Interfaces

Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces with the only noticeable effect being a reduced bandwidth.

This is similar to redundant interfaces with the major difference being that a redundant interface group only uses one link at a time, where an aggregate link group uses the total bandwidth of the functioning links in the group, up to eight (or more).

Support of the IEEE standard 802.3ad for link aggregation is available on some models.

An interface is available to be an aggregate interface if:

- it is a physical interface, not a VLAN interface or subinterface
- it is not already part of an aggregate or redundant interface
- it is in the same VDOM as the aggregated interface. Aggregate ports cannot span multiple VDOMs.
- it does not have an IP address and is not configured for DHCP or PPPoE
- it is not referenced in any security policy, VIP, IP Pool or multicast policy
- it is not an HA heartbeat interface
- it is not one of the FortiGate-5000 series backplane interfaces

Some models of FortiGate units do not support aggregate interfaces. In this case, the aggregate option is not an option in the web-based manager or CLI. As well, you cannot create aggregate interfaces from the interfaces in a switch port.

To see if a port is being used or has other dependencies, use the following diagnose command:

```
diagnose sys checkused system.interface.name <interface_name>
```

When an interface is included in an aggregate interface, it is not listed on the **System > Network > Interface** page. Interfaces will still appear in the CLI, although configuration for those interfaces will not take affect. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, IP pools, or routing.

Example

This example creates an aggregate interface on a FortiGate-3810A using ports 4-6 with an internal IP address of 10.13.101.100, as well as the administrative access to HTTPS and SSH.

To create an aggregate interface - web-based manager

1. Go to **System > Network > Interface** and select **Create New**.
2. Enter the Name as `Aggregate`.
3. For the **Type**, select **802.3ad Aggregate**.
   If this option does not appear, your FortiGate unit does not support aggregate interfaces.
4. In the **Available Interfaces** list, select port 4, 5 and 6 and move it to the **Selected Interfaces** list.
5. Select the **Addressing Mode** of **Manual**.
6. Enter the IP address for the port of 10.13.101.100/24.
7. For **Administrative Access** select HTTPS and SSH.
8. Select **OK**.

To create aggregate interface - CLI

```
config system interface
   edit Aggregate
      set type aggregate
      set member port4 port5 port6
```

```
    set vdom root
    set ip 172.20.120.100/24
    set allowaccess https ssh
end
```

DHCP addressing mode on an interface

If you configure an interface to use DHCP, the FortiGate unit automatically broadcasts a DHCP request from the interface. The interface is configured with the IP address and any DNS server addresses and default gateway address that the DHCP server provides.

DHCP IPv6 is similar to DHCP IPv4, however there is:

- no default gateway option defined because a host learns the gateway using router advertisement messages
- there is no WINS servers because it is obsolete.

For more information about DHCP IPv6, see RFC 3315.

Configure DHCP for an interface in **System > Network > Interface** and selecting the interface from the list, and selecting **DHCP** in the **Address Mode**. The table describes the DHCP status information when DHCP is configured for an interface.

Addressing mode section of New Interface page for DHCP informatio	
Status	Displays DHCP status messages as the interface connects to the DHCP server and gets addressing information. Select **Status** to refresh the addressing mode status message. Status can be one of: • **initializing** - No activity. • **connecting** - interface attempts to connect to the DHCP server. • **connected** - interface retrieves an IP address, netmask, and other settings from the DHCP server. • **failed** - interface was unable to retrieve an IP address and other settings from the DHCP server.
Obtained IP/Netmask	The IP address and netmask leased from the DHCP server. Only displayed if **Status** is **connected**.
Renew	Select to renew the DHCP license for this interface. Only displayed if **Status** is **connected**.
Expiry Date	The time and date when the leased IP address and netmask is no longer valid for the interface. The IP address is returned to the pool to be allocated to the next user request for an IP address. Only displayed if **Status** is **connected**.
Default Gateway	The IP address of the gateway defined by the DHCP server. Only displayed if **Status** is **connected**, and if **Receive default gateway from server** is selected.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route.
Retrieve default gateway from server	Enable to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.
Override internal DNS	Enable to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. When VDOMs are enabled, you can override the internal DNS only on the management VDOM.

PPPoE addressing mode on an interface

If you configure the interface to use PPPoE, the FortiGate unit automatically broadcasts a PPPoE request from the interface.

The FortiGate units support many PPPoE RFC features (RFC 2516) including unnumbered IPs, initial discovery timeout and PPPoE Active Discovery Terminate (PADT).

PPPoE is only configurable in the web-based manager on desktop FortiGate units. 1U FortiGates and up must be configured in the CLI using the commands:

```
config system interface
   edit <port_name>
      set mode pppoe
      set username <ISP_username>
      set password <ISP_password>
      set idle-timeout <seconds>
      set distance <integer>
      set ipunnumbered <unumbered-IP>
      set disc-retry-timeout <seconds>
      set padt-retry-timeout <seconds>
      set lcp-echo-interval <seconds>
      set dns-server-override {enable | disable}
end
```

Configure PPPoE on an interface in **System > Network > Interface**. The table describes the PPPoE status information when PPPoE is configured for an interface.

Addressing mode section of New Interface page	
Status	Displays PPPoE status messages as the FortiGate unit connects to the PPPoE server and gets addressing information. Select Status to refresh the addressing mode status message. The status is only displayed if you selected **Edit**. Status can be any one of the following 4 messages.
Initializing	No activity.
Connecting	The interface is attempting to connect to the PPPoE server.
Connected	The interface retrieves an IP address, netmask, and other settings from the PPPoE server. When the status is connected, PPPoE connection information is displayed.
Failed	The interface was unable to retrieve an IP address and other information from the PPPoE server.
Reconnect	Select to reconnect to the PPPoE server. Only displayed if Status is connected.
User Name	The PPPoE account user name.
Password	The PPPoE account password.
Unnumbered IP	Specify the IP address for the interface. If your ISP has assigned you a block of IP addresses, use one of them. Otherwise, this IP address can be the same as the IP address of another interface or can be any IP address.
Initial Disc Timeout	Enter Initial discovery timeout. Enter the time to wait before starting to retry a PPPoE discovery.
Initial PADT timeout	Enter Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. Set initial PADT timeout to 0 to disable.
Distance	Enter the administrative distance for the default gateway retrieved from the PPPoE server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.

Addressing mode section of New Interface page	
Retrieve default gateway from server	Enable to retrieve a default gateway IP address from a PPPoE server. The default gateway is added to the static routing table.
Override internal DNS	Enable to replace the DNS server IP addresses on the System DNS page with the DNS addresses retrieved from the PPPoE server. When VDOMs are enabled, you can override the internal DNS only on the management VDOM.

Administrative access

Interfaces, especially the public-facing ports can be potentially accessed by those who you may not want access to the FortiGate unit. When setting up the FortiGate unit, you can set the type of protocol an administrator must use to access the FortiGate unit. The options include:

- HTTPS
- HTTP
- SSH
- TELNET
- SNMP
- PING
- FortiManager Access (FMG-Access)
- FortiClient Access (FCT-Access)

You can select as many, or as few, even none, that are accessible by an administrator.

This example adds an IPv4 address 172.20.120.100 to the WAN1 interface as well as the administrative access to HTTPS and SSH. As a good practice, set the administrative access when you are setting the IP address for the port.

To add an IP address on the WAN1 interface - web-based manager

1. Go to **System > Network > Interface**.
2. Select the WAN1 interface row and select **Edit**.
3. Select the **Addressing Mode** of **Manual**.
4. Enter the IP address for the port of 172.20.120.100/24.
5. For **Administrative Access**, select **HTTPS** and **SSH**.
6. Select **OK**.

To create IP address on the WAN1 interface - CLI

```
config system interface
   edit wan1
      set ip 172.20.120.100/24
      set allowaccess https ssh
end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Wireless

A wireless interface is similar to a physical interface only it does not include a physical connection. The FortiWiFi units enables you to add multiple wireless interfaces that can be available at the same time (the FortiWiFi-30B can only have one wireless interface). On FortiWiFi units, you can configure the device to be either an access point, or a wireless client. As an access point, the FortiWiFi unit can have up to four separate SSIDs, each on their own subnet for wireless access. In client mode, the FortiWiFi only has one SSID, and is used as a receiver, to enable remote users to connect to the existing network using wireless protocols.

Wireless interfaces also require additional security measures to ensure the signal does not get hijacked and data tampered or stolen.

For more information on configuring wireless interfaces see the Deploying Wireless Networks Guide.

Interface MTU packet size

You can change the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits to improve network performance. Ideally, the MTU should be the same as the smallest MTU of all the networks between the FortiGate unit and the destination of the packets. If the packets that the FortiGate unit sends are larger than the smallest MTU, they are broken up or fragmented, which slows down transmission. You can easily experiment by lowering the MTU to find an MTU size for optimum network performance.

To change the MTU, select Override default MTU value (1500) and enter the MTU size based on the addressing mode of the interface

- 68 to 1 500 bytes for static mode
- 576 to 1 500 bytes for DHCP mode
- 576 to 1 492 bytes for PPPoE mode
- larger frame sizes if supported by the FortiGate model - up to 9216 bytes for NP2, NP4, and NP6-accelerated interfaces

Only available on physical interfaces. Virtual interfaces associated with a physical interface inherit the physical interface MTU size.

Interfaces on some models support frames larger than the traditional 1500 bytes. Jumbo frames are supported on FortiGate models that have either a SOC2 or NP4lite, except for the FortiGate-30D, as well as on FortiGate-100D series models (for information about your FortiGate unit's hardware, see the Hardware Acceleration guide). For other models, please contact Fortinet Customer Support for the maximum frame size that is supported.

If you need to enable sending larger frames over a route, you need all Ethernet devices on that route to support that larger frame size, otherwise your larger frames will not be recognized and are dropped.

If you have standard size and larger size frame traffic on the same interface, routing alone cannot route them to different routes based only on frame size. However, you can use VLANs to make sure the larger frame traffic is routed over network devices that support that larger size. VLANs will inherit the MTU size from the parent interface. You will need to configure the VLAN to include both ends of the route as well as all switches and routers along the route.

MTU packet size is changed in the CLI. If you select an MTU size larger than your FortiGate unit supports, an error message will indicate this. In this situation, try a smaller MTU size until the value is supported.

In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces on the FortiGate unit to match the new MTU.

To change the MTU size, use the following CLI commands:

```
config system interface
   edit <interface_name>
      set mtu-override enable
      set mtu <byte_size>
end
```

Secondary IP addresses to an interface

If an interface is configured with a manual or static IP address, you can also add secondary static IP addresses to the interface. Adding secondary IP addresses effectively adds multiple IP addresses to the interface. Secondary IP addresses cannot be assigned using DCHP or PPPoE.

All of the IP addresses added to an interface are associated with the single MAC address of the physical interface and all secondary IP addresses are in the same VDOM as the interface that are added to. You configure interface status detection for gateway load balancing separately for each secondary IP addresses. As with all other interface IP addresses, secondary IP addresses cannot be on the same subnet as any other primary or secondary IP address assigned to a FortiGate interface unless they are in separate VDOMs.

To configure a secondary IP, go to **System > Network > Interface**, select **Edit** or **Create New** and select the **Secondary IP Address** check box.

Virtual domains

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. A single FortiGate unit is then flexible enough to serve multiple departments of an organization, separate organizations, or to act as the basis for a service provider's managed security service.

VDOMs provide separate security domains that allow separate zones, user authentication, security policies, routing, and VPN configurations. By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the FortiGate physical interfaces, modem, VLAN subinterfaces, zones, security policies, routing settings, and VPN settings.

When a packet enters a VDOM, it is confined to that VDOM. In a VDOM, you can create security policies for connections between Virtual LAN (VLAN) subinterfaces or zones in the VDOM. Packets do not cross the virtual domain border internally. To travel between VDOMs, a packet must pass through a firewall on a physical interface. The packet then arrives at another VDOM on a different interface, but it must pass through another firewall before entering the VDOM Both VDOMs are on the same FortiGate unit. Inter-VDOMs change this

behavior in that they are internal interfaces; however their packets go through all the same security measures as on physical interfaces.

This example shows how to enable VDOMs on the FortiGate unit and the basic and create a VDOM accounting on the DMZ2 port and assign an administrator to maintain the VDOM. First enable Virtual Domains on the FortiGate unit. When you enable VDOMs, the FortiGate unit will log you out.

For desktop and low-end FortiGate units, VDOMs are enabled using the CLI. On larger FortiGate units, you can enable on the web-based manager or the CLI. Once enabled all further configuration can be made in the web-based manager or CLI.

To enable VDOMs - web-based manager

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select **Enable for Virtual Domain**.

The FortiGate unit logs you out. Once you log back in, you will notice that the menu structure has changed. This reflects the global settings for all Virtual Domains

To enable VDOMs - CLI

```
config system global
   set vdom-admin enable
end
```

Next, add the VDOM called accounting.

To add a VDOM - web-based manager

1. Go to **System > VDOM > VDOM**, and select **Create New**.
2. Enter the VDOM name `accounting`.
3. Select **OK**.

To add a VDOM - CLI

```
config vdom
   edit <new_vdom_name>
end
```

With the Virtual Domain created, you can assign a physical interface to it, and assign it an IP address.

To assign physical interface to the accounting Virtual Domain - web-based manager

1. Go to **System > Network > Interface**.
2. Select the DMZ2 port row and select **Edit**.
3. For the **Virtual Domain** drop-down list, select **accounting**.
4. Select the **Addressing Mode** of **Manual**.
5. Enter the IP address for the port of 10.13.101.100/24.
6. Set the **Administrative Access** to **HTTPS** and **SSH**.
7. Select **OK**.

To assign physical interface to the accounting Virtual Domain - CLI

```
config global
   config system interface
      edit dmz2
         set vdom accounting
         set ip 10.13.101.100/24
         set allowaccess https ssh
   next
end
```

Virtual LANs

The term VLAN subinterface correctly implies the VLAN interface is not a complete interface by itself. You add a VLAN subinterface to the physical interface that receives VLAN-tagged packets. The physical interface can belong to a different VDOM than the VLAN, but it must be connected to a network route that is configured for this VLAN. Without that route, the VLAN will not be connected to the network, and VLAN traffic will not be able to access this interface.The traffic on the VLAN is separate from any other traffic on the physical interface.

FortiGate unit interfaces cannot have overlapping IP addresses, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask. This rule helps prevent a broadcast storm or other similar network problems.

Any FortiGate unit, with or without VDOMs enabled, can have a maximum of 255 interfaces in Transparent operating mode. In NAT/Route operating mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in Transparent operating mode, you need to configure multiple VDOMs with many interfaces on each VDOM.

This example shows how to add a VLAN, vlan_accounting on the FortiGate unit internal interface with an IP address of 10.13.101.101.

To add a VLAN - web-based manager

1. Go to **System > Network > Interface** and select **Create New**.
   The **Type** is by default set to VLAN.
2. Enter a name for the **VLAN** to `vlan_accounting`.
3. Select the **Internal** interface.
4. Enter the **VLAN ID**.
   The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together.
5. Select the **Addressing Mode** of **Manual**.
6. Enter the IP address for the port of 10.13.101.101/24.
7. Set the **Administrative Access** to **HTTPS** and **SSH**.
8. Select **OK**.

To add a VLAN - CLI

```
config system interface
```

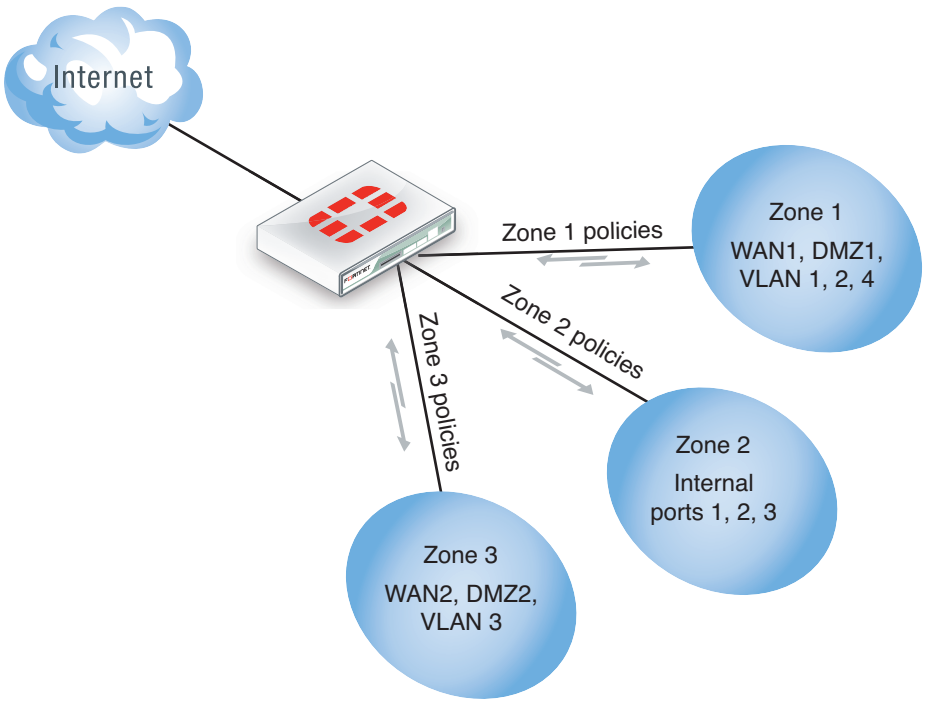
```
    edit VLAN_1
       set interface internal
       set type vlan
       set vlanid 100
       set ip 10.13.101.101/24
       set allowaccess https ssh
    next
end
```

Zones

Zones are a group of one or more FortiGate interfaces, both physical and virtual, that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each interface still has its own address and routing is still done between interfaces, that is, routing is not affected by zones. Security policies can also be created to control the flow of intra-zone traffic.

For example, in the illustration below, the network includes three separate groups of users representing different entities on the company network. While each group has its own set of port and VLANs, in each area, they can all use the same security policy and protection profiles to access the Internet. Rather than the administrator making nine separate security policies, he can add the required interfaces to a zone, and create three policies, making administration simpler.

Network zones



You can configure policies for connections to and from a zone, but not between interfaces in a zone. Using the above example, you can create a security policy to go between zone 1 and zone 3, but not between WAN2 and WAN1, or WAN1 and DMZ1.

This example explains how to set up a zone to include the Internal interface and a VLAN.

To create a zone - web-based manager

1. Go to **System > Network > Interface**.
2. Select the arrow on the **Create New** button and select **Zone**.
3. Enter a zone name of `Zone_1`.
4. Select the Internal interface and the virtual LAN interface **vlan_accounting** created previously.
5. Select **OK**.

To create a zone - CLI

```
config system zone
   edit Zone_1
      set interface internal VLAN_1
end
```

Probing interfaces

Server probes can be used on interfaces. In order for this to occur, the probe response mode must first be configured, then the probe response must be allowed administrative access on the interface. The probe response mode can be:

`none`	Disable probe.
`http-probe`	HTTP probe.
`twamp`	Two way active measurement protocol.

Both steps must be done through the CLI.

Configuring the probe

```
config system probe-response
   set mode http-probe
end
```

Allowing the probe response to have administrative access to the interface

```
config system interface
   edit <port>
      set allowaccess probe-response
   end
end
```

Central management

Administering one or two FortiGate units is fairly simple enough, especially when they are in the same room or building. However, if you are administering many FortiGate units that may be located in locations in a large geographical area, or in the world, you will need a more efficient method of maintaining firmware upgrades, configuration changes, and updates.

The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances. FortiManager appliances provide centralized policy-based provisioning, configuration, and update management, as well as end-to-end network monitoring for added control. Managers can control administrative access and simplify policy deployment using role-based administration to define user privileges for specific management domains and functions by aggregating collections of Fortinet appliances and agents into independent management domains. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response time and maximize network protection.

This chapter describes the basics of using FortiManager as an administration tool for multiple FortiGate units. It describes the basics of setting up a FortiGate unit in FortiManager and some key management features you can use within FortiManager to manage the FortiGate unit. For full details and instructions on FortiManager, see the FortiManager Administration Guide.

This section includes the topics:

- Adding a FortiGate to FortiManager
- Configuration through FortiManager
- Firmware updates
- FortiGuard
- Backup and restore configurations
- Administrative domains

In order for the FortiGate unit and FortiManager unit to properly connect, both units must have compatible firmware. To find out if your firmware is compatible, refer to the FortiOS or FortiManager Release Notes.

Adding a FortiGate to FortiManager

Before you can maintain a FortiGate unit using a FortiManager unit, you need to add it to the FortiManager. This requires configuration on both the FortiGate and FortiManager. This section describes the basics to configure management using a FortiManager device. For more information on the interaction of FortiManager with the FortiGate unit, see the FortiManager documentation.

FortiGate configuration

These steps ensure that the FortiGate unit will be able to receive updated antivirus and IPS updates and allow remote management through the FortiManager system. You can add a FortiGate unit whether it is running in either NAT mode or transparent mode. The FortiManager unit provides remote management of a FortiGate unit over TCP port 541.

If you have not already done so, register the FortiGate unit by visiting http://support.fortinet.com and select **Product Registration**. By registering your Fortinet unit, you will receive updates to threat detection and prevention databases (Antivirus, Intrusion Detection, etc.) and will also ensure your access to technical support.

You must enable the FortiGate management option so the FortiGate unit can accept management updates to firmware, antivirus signatures, and IPS signatures.

To configure the FortiGate unit - web-based manager

1. Log in to the FortiGate unit.
2. Go to **System > Admin > Settings**.
3. Enter the **IP address** for the FortiManager unit.
4. Select **Send Request**.

The FortiManager ID now appears in the Trusted FortiManager table.

As an additional security measure, you can also select **Registration Password** and enter a password to concon nect to the FortiManager.

To configure the FortiGate unit - CLI

```
config system central-management
   set fmg <ip_address>
end
```

To use the registration password enter:

```
execute central-mgmt register-device <fmg-serial-no><fmg-register-password><fgt-
    usrname><fgt-password>
```

Configuring an SSL connection

An SSL connection can be configured between the two devices and an encryption level selected. Use the following CLI commands in the FortiGate CLI to configure the connection:

```
config system central-management
   set status enable
   set enc-algorithm {default* | high | low}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- **High** - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA

- **Medium** - Key strengths of 128 bit encryption.

Algorithms are: RC4-SHA:RC4-MD5:RC4-MD

- **Low** - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites

Algorithms are: EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

FortiManager configuration

Once the connection between the FortiGate unit and the FortiManager unit has been configured, you can add the FortiGate to the Device Manager in the FortiManager unit's web-based manager. For details on completing the configuration, see the FortiManager Administration Guide.

Configuration through FortiManager

With the FortiManager system, you can monitor and configure multiple FortiGate units from one location. Using the FortiManager's Device Manager, you can view the FortiGate units and make the usual configuration updates and changes, without having to log in and out of multiple FortiGate units.

FortiManager enables you to complete the configuration, by going to the Device Manager, selecting the FortiGate unit and using the same menu structure and pages as you would see in the FortiGate web-based manager. All changes to the FortiGate configuration are stored locally on the FortiManager unit until you synchronize with the FortiGate unit.

When a FortiGate unit is under control of a FortiManager system, administrators will not be able to change the configuration using the FortiGate. When trying to change options, the unit displays a message that it is configured through FortiManager, and any changes may be reverted.

Global objects

If you are maintaining a number of FortiGate units within a network, many of the policies and configuration elements will be the same across the corporation. In these instances, the adding and editing of many of the same policies will be come a tedious and error-prone activity. With FortiManager global objects, this level of configuration is simplified.

A global object is an object that is not associated specifically with one device or group. Global objects includes security policies, a DNS server, VPN, and IP pools.

The Global Objects window is where you can configure global objects and copy the configurations to the FortiManager device database for a selected device or a group of devices. You can also import configurations from the FortiManager device database for a selected device and modify the configuration as required.

When configuring or creating a global policy object the interface, prompts, and fields are the same as creating the same object on a FortiGate unit using the FortiGate web-based manager.

Locking the FortiGate web-based manager

When you use the FortiManager to manager multiple FortiGate units, a local FortiGate unit becomes locked from any configuration changes using the web-based manager for most administrators. The super_admin will still be able to make changes to the configuration; however, this is not recommended as it may cause conflicts with the FortiManager.

Firmware updates

A FortiManager unit can also perform firmware updates for multiple FortiGate units, saving time rather than upgrading each FortiGate unit individually.

The FortiManager unit stores local copies of firmware images, either by downloading images from the Fortinet Distribution Network (FDN) or by accepting firmware images that are uploaded from the management computer.

If you are using the FortiManager unit to download firmware images, the FDN first validates device licenses and support contracts and then provides a list of currently available firmware images. For devices with valid Fortinet Technical Support contracts, you can download new firmware images from the FDN and the firmware release notes.

After firmware images have been either downloaded from the FDN or imported to the firmware list, you can either schedule or immediately upgrade/downgrade a device or group of device's firmware.

See the FortiManager Administration Guide for more information on updating the FortiGate firmware using the FortiManager central management.

FortiGuard

FortiManager can also connect to the FortiGuard Distribution Network (FDN) to receive push updates for IPS signatures and antivirus definitions. These updates can then be used to update multiple FortiGate units throughout an organization. By using the FortiManager as the host for updates, bandwidth use is minimized as updates are downloaded to one source instead of many.

To receive IPS and antivirus updates from FortiManager, indicate an alternate IP address on the FortiGate unit.

To configure updates from FortiManager

1. Go to **System > Config > FortiGuard**.
2. Select **AntiVirus and IPS Options** to expand the options.
3. Enable both **Allow Push Update** and **Use override push IP**.
4. Enter the IP address of the FortiManager unit.
5. Select **Apply**.

Backup and restore configurations

A FortiManager unit stores configuration files for backup and restore purposes. A FortiManager also enables you to save revisions of configuration files. Configuration backups occur automatically when the administrator logs out or the administrator login session expires.

FortiManager also enables you to view differences between different configurations to view where changes have been made.

Administrative domains

FortiManager administrative domains enable the super_admin to create groupings of devices for configured administrators to monitor and manage. FortiManager can manage a large number of Fortinet appliances. This enables administrators to maintain managed devices specific to their geographic location or business division. This also includes FortiGate units with multiple configured VDOMs.

Each administrator is tied to an administrative domain (ADOM). When that particular administrator logs in, they see only those devices or VDOMs configured for that administrator and ADOM. The one exception is the super_admin account that can see and maintain all administrative domains and the devices within those domains.

Administrative domains are not enabled by default and enabling and configuring the domains can only be performed by the super_admin.

The maximum number of administrative domains you can add depends on the FortiManager system model. See the FortiManager Administration Guide for information on the maximums for each model.

Monitoring

With network administration, the first step is installing and configuring the FortiGate unit to be the protector of the internal network. Once the system is running efficiently, the next step is to monitor the system and network traffic, making configuration changes as necessary when a threat or vulnerability is discovered.

This chapter discusses the various methods of monitoring both the FortiGate unit and the network traffic through a range of different tools available within FortiOS.

This section includes the topics:

- Dashboard
- sFlow
- Monitor menus
- Logging
- Alert email
- SNMP
- SNMP get command syntax

Dashboard

The FortiOS dashboard provides a location to view real-time system information. By default, the dashboard displays the key statistics of the FortiGate unit itself, providing the memory and CPU status, as well as the health of the ports, whether they are up or down and their throughput.

Widgets

Within the dashboard is a number of smaller windows, called widgets, that provide this status information. Beyond what is visible by default, you can add a number of other widgets that display other key traffic information including application use, traffic per IP address, top attacks, traffic history and logging statistics.

You can add multiple dashboards to reflect what data you want to monitor, and add the widgets accordingly. Dashboard configuration is only available through the web-based manager. Administrators must have read and write privileges to customize and add widgets when in either menu. Administrators must have read privileges if they want to view the information.

To add a dashboard and widgets

1. Go to **System > Dashboard > Status**.
2. Select the **Dashboard** menu at the top of the window and select **Add Dashboard**.
3. Enter a name.
4. Select the **Widget** menu at the top of the window.
5. From the screen, select the type of information you want to add.
6. When done, select the X in the top right of the widget.

Dashboard widgets provide an excellent method to view real-time data about the events occurring on the FortiGate unit and the network. For example, by adding the Network Protocol Usage widget, you can monitor the

activity of various protocols over a selected span of time. Based on that information you can add or adjust traffic shaping and/or security policies to control traffic.

FortiClient software

The **License Information** widget includes information for the FortiClient connections. It displays the number of FortiClient connections allowed and the number of users connecting. By selecting the **Details** link for the number of connections, you can view more information about the connecting user, including IP address, user name, and type of operating system the user is connecting with.

Included with this information is a link for Mac and Windows. Selecting these links automatically downloads the FortiClient install file (.dmg or .exe) to the management computer.

sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that may impact performance and throughput. FortiOS implements sFlow version 5.

sFlow uses packet sampling to monitor network traffic. The sFlow Agent captures packet information at defined intervals and sends them to an sFlow Collector for analysis, providing real-time data analysis. The information sent is only a sampling of the data for minimal impact on network throughput and performance.

The sFlow Agent is embedded in the FortiGate unit. Once configured, the FortiGate unit sends sFlow datagrams of the sampled traffic to the sFlow Collector, also called an sFlow Analyzer. The sFlow Collector receives the datagrams, and provides real-time analysis and graphing to indicate where potential traffic issues are occurring. sFlow Collector software is available from a number of third party software vendors.

sFlow data captures only a sampling of network traffic, not all traffic like the traffic logs on the FortiGate unit. Sampling works by the sFlow Agent looking at traffic packets when they arrive on an interface. A decision is made whether the packet is dropped and allowed to be to its destination or if a copy is forwarded to the sFlow Collector. The sample used and its frequency are determined during configuration.

sFlow is not supported on virtual interfaces such as vdom link, ipsec, ssl.root or gre.

The sFlow datagram sent to the Collector contains the information:

- Packet header (e.g. MAC,IPv4,IPv6,IPX,AppleTalk,TCP,UDP, ICMP)
- Sample process parameters (rate, pool etc.)
- Input/output ports
- Priority (802.1p and TOS)
- VLAN (802.1Q)
- Source/destination prefix
- Next hop address
- Source AS, Source Peer AS
- Destination AS Path
- Communities, local preference
- User IDs (TACACS/RADIUS) for source/destination
- URL associated with source/destination
- Interface statistics (RFC 1573, RFC 2233, and RFC 2358)

sFlow agents can be added to any type of FortiGate interface. sFlow isn't supported on some virtual interfaces such as VDOM link, IPsec, gre, and ssl.root.

For more information on sFlow, Collector software and sFlow MIBs, visit www.sflow.org.

Configuration

sFlow configuration is available only from the CLI. Configuration requires two steps: enabling the sFlow Agent and configuring the interface for the sampling information.

Enable sFlow

```
config system sflow
   set collector-ip <ip_address>
   set collector-port <port_number>
   set source-ip <ip_address>
end
```

The default port for sFlow is UDP 6343. To configure in VDOM, use the commands:

```
config system vdom-sflow
   set vdom-sflow enable
   set collector-ip <ip_address>
   set collector-port <port_number>
   set source-ip <ip_address>
end
```

Configure sFlow agents per interface.

```
config system interface
   edit <interface_name>
      set sflow-sampler enable
      set sample-rate <every_n_packets>
      set sample-direction [tx | rx | both]
      set polling-interval <seconds>
   end
```

Monitor menus

The **Monitor** menus enable you to view session and policy information and other activity occurring on your FortiGate unit. The monitors provide the details of user activity, traffic and policy usage to show live activity. Monitors are available for DHCP, routing, security policies, traffic shaping, load balancing, security features, VPN, users, WiFi, and logging.

Logging

FortiOS provides a robust logging environment that enables you to monitor, store, and report traffic information and FortiGate events, including attempted log ins and hardware status. Depending on your requirements, you can log to a number of different hosts.

To configure logging in the web-based manager, go to **Log & Report > Log Config > Log Settings**.

To configure logging in the CLI use the commands `config log <log_location>`.

For details on configuring logging see the Logging and Reporting Guide.

If you will be using several FortiGate units, you can also use a FortiAnalyzer unit for logging. For more information, see the FortiAnalyzer Administration Guide.

FortiCloud

The FortiCloud is a subscription-based hosted service. With this service, you can have centralized management, logging, and reporting capabilities available in FortiAnalyzer and FortiManager platforms, without any additional hardware to purchase, install or maintain. In most cases, FortiCloud is the recommended location for saving and viewing logs.

This service includes a full range of reporting, analysis and logging, firmware management and configuration revision history. It is hosted within the Fortinet global FortiGuard Network for maximum reliability and performance, and includes reporting, and drill-down analysis widgets makes it easy to develop custom views of network and security events.

The FortiGate unit sends log messages to the FortiCloud using TCP port 443. Configuration is available once a user account has been set up and confirmed. To enable the account on the FortiGate unit, go to **System > Dashboard > Status**, in the **Licence Information** widget select **Activate**, and enter the account ID.

For FortiCloud traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of the FortiCloud server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log fortiguard setting
   set status enable
   set source-ip 192.168.4.5
end
```

From the FortiGate unit, you can configure the connection and sending of log messages to be sent over an SSL tunnel to ensure log messages are sent securely. To do this, use the CLI commands to enable the encrypted connection and define the level of encryption.

```
config log fortiguard setting
   set status enable
   set enc-alogorithm {default | high | low | disable}
end
```

FortiGate memory

Logs are saved to the internal memory by default. Inexpensive yet volatile, for basic event logs or verifying traffic, AV or spam patterns, logging to memory is a simple option. However, because logs are stored in the limited space of the internal memory, only a small amount is available for logs. As such logs can fill up and be overridden with new entries, negating the use of recursive data. This is especially true for traffic logs. Also, should the FortiGate unit be shut down or rebooted, all log information will be lost.

FortiGate hard disk

For those FortiGate units with an internal hard disk or SDHC card, you can store logs to this location. Efficient and local, the hard disk provides a convenient storage location. If you choose to store logs in this manner, remember to backup the log data regularly.

Configure log disk settings is performed in the CLI using the commands:

```
config log disk setting
   set status enable
end
```

Further options are available when enabled to configure log file sizes, and uploading/backup events.

As well, note that the write speeds of hard disks compared to the logging of ongoing traffic may cause the dropping such, it is recommended that traffic logging be sent to a FortiAnalyzer or other device meant to handle large volumes of data.

Syslog server

An industry standard for collecting log messages, for off-site storage. In the web-based manager, you are able to send logs to a single syslog server, however in the CLI you can configure up to three syslog servers where you can also use multiple configuration options. For example, send traffic logs to one server, antivirus logs to another. The FortiGate unit sends Syslog traffic over UDP port 514. Note that if a secure tunnel is configured for communication to a FortiAnalyzer unit, then Syslog traffic will be sent over an IPsec connection, using UPD 500/4500, Protocol IP/50.

To configure a Syslog server in the web-based manager, go to **Log & Report > Log Config > Log Settings**. In the CLI use the commands:

```
config log syslogd setting
   set status enable
   set server <IP address or FQDN of syslog server>
end
```

Further options are available when enabled to configure a different port, facility and server IP address.

For Syslog traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a Syslog server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log syslogd setting
   set status enable
   set source-ip 192.168.4.5
end
```

FortiAnalyzer

The FortiAnalyzer family of logging, analyzing, and reporting appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, users can filter and review records, including traffic, event, virus, attack, Web content, and email data, mining the data to determine your security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, Web access, instant messaging and file transfer content.

The FortiGate unit sends log messages over UDP port 514 or OFTP (TCP 514). If a secure connection has been configured, log traffic is sent over UDP port 500/4500, Protocol IP/50.

For FortiAnalyzer traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command set `source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a FortiAnalyzer unit to be on port 3 with an IP of 192.168.21.12, the commands are:

```
config log fortiguard setting
   set status enable
   set source-ip 192.168.21.12
end
```

Sending logs using a secure connection

From the FortiGate unit, you can configure the connection and sending of log messages over an SSL tunnel to ensure log messages are sent securely. To do this, use the CLI commands below to enable the encrypted connection and define the level of encryption.

You must configure the secure tunnel on **both** ends of the tunnel, the FortiGate unit and the FortiAnalyzer unit.

To configure a secure connection to the FortiAnalyzer unit

On the FortiAnalyzer unit, enter the commands:

```
config log device
   edit <device_name>
      set secure psk
      set psk <name_of_IPsec_tunnel>
      set id <fortigate_device_name_on_the_fortianalyzer>
end
```

To configure a secure connection on the FortiGate unit

On the FortiGate CLI, enter the commands:

```
config log fortianalyzer setting
   set status enable
   set server <ip_address>
   set localid <name_of_IPsec_tunnel>
end
```

Configuring an SSL connection

An SSL connection can be configured between the two devices, and an encryption level selected.

Use the CLI commands to configure the encryption connection:

```
config log fortianalyzer setting
   set status enable
   set enc-algorithm {default* | high | low | disable}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- **High** - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA

- **Medium** - Key strengths of 128 bit encryption.

Algorithms are: RC4-SHA:RC4-MD5:RC4-MD

- **Low** - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites

Algorithms are: EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

If you want to use an IPsec tunnel to connect to the FortiAnalyzer unit, you need to first disable the enc-algorithm:

```
config log fortianalyzer setting
   set status enable
   set enc-algorithm disable
```

Then set the IPsec encryption:

```
set encrypt enable
   set psksecret <preshared_IPsec_tunnel_key>
end
```

Packet Capture

When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture can also be called a network tap, packet sniffing, or logic analyzing.

To use the packet capture.

1. Go to **System > Network > Packet Capture**.
2. Select **Create New** or an existing entry is there is one that meets your needs.
3. Select the interface to monitor and select the number of packets to keep.
4. Select **Enable Filters**.
5. Enter the information you want to gather from the packet capture.
6. Select **OK**.

To run the capture, select the play button in the progress column in the packet capture list. If not active, **Not Running** will also appear in the column cell. The progress bar will indicate the status of the capture. You can stop and restart it at any time.

When the capture is complete, select the **Download** icon to save the packet capture file to your hard disk for further analysis.

Packet capture tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- finding missing traffic
- seeing if sessions are setting up properly
- locating ARP problems such as broadcast storm sources and causes
- confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks
- confirming routing is working as you expect
- wireless client connection problems
- intermittent missing PING packets
- a particular type of packet is having problems, such as UDP, which is commonly used for streaming video

If you are running a constant traffic application such as ping, packet capture can tell you if the traffic is reaching the destination, how the port enters and exits the FortiGate unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start capturing packets, you need to have a good idea of what you are looking for. Capture is used to confirm or deny your ideas about what is happening on the network. If you try capture without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to capture enough packets to really understand all of the patterns and behavior that you are looking for.

Alert email

As an administrator, you want to be certain you can respond quickly to issues occurring on your network or on the FortiGate unit. Alert emails provide an efficient and direct method of notifying an administrator of events. By configuring alert messages, you can define the threshold when a problem becomes critical and needs attention. When this threshold is reached, the FortiGate unit will send an email to one or more individuals, notifying them of the issue.

In the following example, the FortiGate unit is configured to send email to two administrators (admin1 and admin2) when multiple intrusions are detected every two minutes. The FortiGate unit has its own email address on the mail server.

To configure the email service

1. Go to **System > Config > Advanced**.
2. In the **Email Service**, complete the following and select **Apply**:

SMTP Server	Enter the address or name of the email server. For example, `smtp.example.com`.
Default Reply To	Enter an email address to associate with the alert email. This field is optional. If you enter an email address here, it overrides the email address entered when configuring alert email in **Log & Report > Alert E-mail**.
Authentication	Enable authentication if required by the email server.
Security mode	Choose between *None*, *SMTPS* or *STARTTLS*
Port	25

To configure alert email - web-based manager

1. Go to **Log & Report > Log Config > Alert E-mail**.
2. Enter the information:

Email from	fortigate@example.com
Email to	admin1@example.com admin2@example.com

3. For the **Interval Time**, enter 2.
4. Select **Intrusion Detected**.
5. Select **Apply**.

To configure alert email - CLI

```
config system email-server
   set port 25
   set server smtp.example.com
   set authenticate enable
   set username FortiGate
   set password *************
end
config alertemail setting
   set username fortigate@example.com
   set mailto1 admin1@example.com
   set mailto2 admin2@example.com
   set filter category
   set IPS-logs enable
end
```

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is a typically a computer running an application that can read the incoming trap and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiGate units. FortiOS supports SNMP using IPv4 and IPv6 addressing.

By using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that FortiGate unit or be able to query that unit.

The FortiGate SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiGate system information through queries and can receive trap messages from the FortiGate unit.

To monitor FortiGate system information and receive FortiGate traps, you must first compile the Fortinet and FortiGate Management Information Base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiGate unit SNMP agent.

FortiGate core MIB files are available for download by going to **System > Config > SNMP** and selecting the download link on the page.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see “Fortinet MIBs”. RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to events that occur such as an a full log disk or a virus detected.

SNMP fields contain information about the FortiGate unit, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

The FortiGate SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI. See the `system snmp user` command in the FortiGate CLI Reference.

SNMP configuration settings

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections by going to **System > Network > Interface**. Select the interface and, in the **Administrative Access**, select **SNMP**.

For VDOMS, SNMP traps can only be sent on interfaces in the management VDOM. Traps cannot be sent over other interfaces outside the management VDOM.

To configure SNMP settings, go to **System > Config > SNMP**.

SNMP Agent	Select to enable SNMP communication.
Description	Enter descriptive information about the FortiGate unit. The description can be up to 35 characters.
Location	Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long.
Contact	Enter the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters.
SNMP v1/v2c section To create a new SNMP community, see SNMP Community page.	
Community Name	The name to identify the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates traps are enabled; a gray x indicates traps are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Enable	Select the check box to enable or disable the community.
SNMP v3 section To create a new SNMP community, see SNMP Community pager.	
User Name	The name of the SNMPv3 user.
Security Level	The security level of the user.
Notification Host	The IP address or addresses of the host.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled
New SNMP Community page	
Community Name	Enter a name to identify the SNMP community
Hosts (section)	

IP Address	Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Interface	Optionally, select the name of the interface that this SNMP manager uses to connect to the FortiGate unit. You only have to select the interface if the SNMP manager is not on the same subnet as the FortiGate unit. This can occur if the SNMP manager is on the Internet or behind a router. In virtual domain mode, the interface must belong to the management VDOM to be able to pass SNMP traps.
Delete	Removes an SNMP manager from the list within the **Hosts** section.
Add	Select to add a blank line to the Hosts list. You can add up to eight SNMP managers to a single community.
Queries (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.
Enable	Select to enable that SNMP protocol.
Traps (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Local	Enter the remote port numbers (port 162 for each by default) that the FortiGate unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. Select the **Enable** check box to activate traps for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for traps.

Remote	Enter the remote port number (port 162 is default) that the FortiGate unit uses to send SNMP v1 or v2c traps to the SNMP managers in this community. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.
Enable	Select to activate traps for each SNMP version.
SNMP Event	Enable each SNMP event for which the FortiGate unit should send traps to the SNMP managers in this community. **CPU Over usage** traps sensitivity is slightly reduced, by spreading values out over 8 polling cycles. This prevents sharp spikes due to CPU intensive short-term events such as changing a policy. **Power Supply Failure** event trap is available only on some models. **AMC interfaces enter bypass mode** event trap is available only on models that support AMC modules.
Enable	Select to enable the SNMP event.
Create New SNMP V3 User	
User Name	Enter the name of the user.
Security Level	Select the type of security level the user will have.
Notification Host	Enter the IP address of the notification host. If you want to add more than one host, after entering the IP address of the first host, select the plus sign to add another host.
Enable Query	Select to enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the field.
Events	Select the SNMP events that will be associated with that user.

Gigabit interfaces

When determining the interface speed of a FortiGate unit with a 10G interface, the IF-MIB.ifSpeed may not return the correct value. IF-MIB.ifSpeed is a 32-bit gauge used to report interface speeds in bits/second and cannot convert to a 64-bit value. The 32-bit counter wrap the output too fast to be accurate.

In this case, you can use the value ifHighSpeed. It reports interface speeds in megabits/second. This ensures that 10Gb interfaces report the correct value.

SNMP agent

You need to first enter information and enable the FortiGate SNMP Agent. Enter information about the FortiGate unit to identify it so that when your SNMP manager receives traps from the FortiGate unit, you will know which

unit sent the information.

To configure the SNMP agent - web-based manager

1. Go to **System > Config > SNMP**.
2. Select **Enable** for the **SNMP Agent**.
3. Enter a descriptive name for the agent.
4. Enter the location of the FortiGate unit.
5. Enter a contact or administrator for the SNMP Agent or FortiGate unit.
6. Select **Apply**.

To configure SNMP agent - CLI

```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiGate>
   set location <FortiGate_location>
end
```

SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiGate unit so that SNMP managers can connect to view system information and receive SNMP traps.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

When the FortiGate unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain. Traps cannot be sent over other interfaces.

To add an SNMP v1/v2c community - web-based manager

1. Go to **System > Config > SNMP**.
2. In the **SNMP v1/v2c** area, select **Create New**.
3. Enter a **Community Name**.
4. Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
5. Select the interface if the SNMP manager is not on the same subnet as the FortiGate unit.
6. Enter the **Port** number that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version.
7. Enter the Local and Remote port numbers that the FortiGate unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community.

8. Select the **Enable** check box to activate traps for each SNMP version.
9. Select **OK**.

To add an SNMP v1/v2c community - CLI

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-lport <port_number>
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_number>
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
end
```

To add an SNMP v3 community - web-based manager

1. Go to **System > Config > SNMP**.
2. In the **SNMP v3** area, select **Create New**.
3. Enter a **User Name**.
4. Select a **Security Level** and associated authorization algorithms.
5. Enter the IP address of the **Notification Host** SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
6. Enter the **Port** number that the SNMP managers in this community use to receive configuration information from the FortiGate unit. Select the **Enable** check box to activate queries for each SNMP version.
7. Select the **Enable** check box to activate traps.
8. Select **OK**.

To add an SNMP v3 community - CLI

```
config system snmp user
   edit <index_number>
      set security-level [auth-priv | auth-no-priv | no-auth-no-priv}
      set queries enable
      set query-port <port_number>
      set notify-hosts <ip_address>
      set events <event_selections>
end
```

Enabling on the interface

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

To configure SNMP access - web-based manager

1. Go to **System > Network > Interface**.
2. Choose an interface that an SNMP manager connects to and select **Edit**.
3. In **Administrative Access**, select **SNMP**.
4. Select **OK**.

To configure SNMP access - CLI

```
config system interface
   edit <interface_name>
      set allowaccess snmp
end
```

If the interface you are configuring already has protocols that are allowed access, use the command `append allowaccess snmp` instead, or else the other protocols will be replaced. For more information, see Adding and removing options from lists.

Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

There are two MIB files for FortiGate units - the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields and information that is specific to FortiGate units. Each Fortinet product has its own MIB. If you use other Fortinet products you will need to download their MIB files as well. Both MIB files are used for FortiOS and FortiOS Carrier; there are no additional traps for the Carrier version of the operating system.

The Fortinet MIB and FortiGate MIB along with the two RFC MIBs are listed in tables in this section. You can download the two FortiGate MIB files from Fortinet Customer Support. The Fortinet MIB contains information for Fortinet products in general. the Fortinet FortiGate MIB includes the system information for The FortiGate unit and version of FortiOS. Both files are required for proper SNMP data collection.

To download the MIB files, go to **System > Config > SNMP** and select a MIB link in the **FortiGate SNMP MIB** section.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet specific information.

There were major changes to the MIB files between FortiOS Carrier v3.0 and v4.0. You need to use the new MIBs for FortiOS Carrier v4.0 or you may mistakenly access the wrong traps and fields.

MIB files are updated for each version of FortiOS. When upgrading the firmware ensure that you updated the Fortinet FortiGate MIB file as well.

Fortinet MIBs

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiGate unit configuration settings and receive traps from the FortiGate SNMP agent.
FORTINET-FORTIGATE-MIB.mib	The FortiGate MIB includes all system configuration information and trap information that is specific to FortiGate units. Your SNMP manager requires this information to monitor FortiGate configuration settings and receive traps from the FortiGate SNMP agent. FortiManager systems require this MIB to monitor FortiGate units.
RFC-1213 (MIB II)	The FortiGate SNMP agent supports MIB II groups with these exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The FortiGate SNMP agent supports Ethernet-like MIB information. FortiGate SNMP does not support for the dot3Tests and dot3Errors groups.

SNMP get command syntax

Normally, to get configuration and status information for a FortiGate unit, an SNMP manager would use an SNMP get commands to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

…where…

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. The most commonly used community name is `public`.

`<address_ipv4>` is the IP address of the FortiGate interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself.

The SNMP `get` command gets firmware version running on the FortiGate unit. The community name is `public`. The IP address of the interface configured for SNMP management access is `10.10.10.1`. The firmware version MIB field is `fgSysVersion` and the OID for this MIB field is `1.3.6.1.4.1.12356.101.4.1.1` The first command uses the MIB field name and the second uses the OID:

```
snmpget -v2c -c public 10.10.10.1 fgSysVersion.0
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.4.1.1.0
```

The OIDs and object names used in these examples are dependent on the version of MIB and are subject to change.

VLANs

Virtual Local Area Networks (VLANs) multiply the capabilities of your FortiGate unit, and can also provide added network security. Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

A Local Area Network (LAN) is a group of connected computers and devices that are arranged into network broadcast domains. A LAN broadcast domain includes all the computers that receive a packet broadcast from any computer in that broadcast domain. A switch will automatically forward the packets to all of its ports; in contrast, routers do not automatically forward network broadcast packets. This means routers separate broadcast domains. If a network has only switches and no routers, that network is considered one broadcast domain, no matter how large or small it is. Smaller broadcast domains are more efficient because fewer devices receive unnecessary packets. They are more secure as well because a hacker reading traffic on the network will have access to only a small portion of the network instead of the entire network's traffic.

Virtual LANs (VLANs) use ID tags to logically separate a LAN into smaller broadcast domains. Each VLAN is its own broadcast domain. Smaller broadcast domains reduce traffic and increase network security. The IEEE 802.1Q standard defines VLANs. All layer-2 and layer-3 devices along a route must be 802.1Q-compliant to support VLANs along that route.

VLANs reduce the size of the broadcast domains by only forwarding packets to interfaces that are part of that VLAN or part of a VLAN trunk link. Trunk links form switch-to-switch or switch-to-router connections, and forward traffic for all VLANs. This enables a VLAN to include devices that are part of the same broadcast domain, but physically distant from each other.

VLAN ID tags consist of a 4-byte frame extension that switches and routers apply to every packet sent and received in the VLAN. Workstations and desktop computers, which are commonly originators or destinations of network traffic, are not an active part of the VLAN process. All the VLAN tagging and tag removal is done after the packet has left the computer.

Any FortiGate unit without VDOMs enabled can have a maximum of 255 interfaces in transparent operating mode. The same is true for any single VDOM. In NAT mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in transparent operating mode, you need to configure multiple VDOMs that enable you to divide the total number of interfaces over all the VDOMs.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

This guide uses the term "packet" to refer to both layer-2 frames and layer-3 packets.

VLAN ID rules

Layer-2 switches and layer-3 devices add VLAN ID tags to the traffic as it arrives and remove them before they deliver the traffic to its final destination. Devices such as PCs and servers on the network do not require any

special configuration for VLANs. Twelve bits of the 4-byte VLAN tag are reserved for the VLAN ID number. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.

On a layer-2 switch, you can have only one VLAN subinterface per physical interface, unless that interface is configured as a trunk link. Trunk links can transport traffic for multiple VLANs to other parts of the network.

On a FortiGate unit, you can add multiple VLANs to the same physical interface. However, VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID or have IP addresses on the same subnet. You can add VLAN subinterfaces with the same VLAN ID to different physical interfaces.

Creating VLAN subinterfaces with the same VLAN ID does not create any internal connection between them. For example a VLAN ID of 300 on port1 and VLAN ID of 300 on port2 are allowed, but they are not connected. Their relationship is the same as between any two FortiGate network interfaces.

VLAN switching and routing

VLAN switching takes place on the OSI model layer-2, just like other network switching. VLAN routing takes place on the OSI model layer-3. The difference between them is that during VLAN switching, VLAN packets are simply forwarded to their destination. This is different from VLAN routing where devices can open the VLAN packets and change their VLAN ID tags to route the packets to a new destination.

VLAN layer-2 switching

Ethernet switches are layer-2 devices, and generally are 802.1Q compliant. Layer 2 refers to the second layer of the seven layer Open Systems Interconnect (OSI) basic networking model; the Data Link layer. FortiGate units act as layer-2 switches or bridges when they are in transparent mode. The units simply tag and forward the VLAN traffic or receive and remove the tags from the packets. A layer-2 device does not inspect incoming packets or change their contents; it only adds or removes tags and routes the packet.

A VLAN can have any number of physical interfaces assigned to it. Multiple VLANs can be assigned to the same physical interface. Typically two or more physical interfaces are assigned to a VLAN, one for incoming and one for outgoing traffic. Multiple VLANs can be configured on one FortiGate unit, including trunk links.

Layer-2 VLAN example

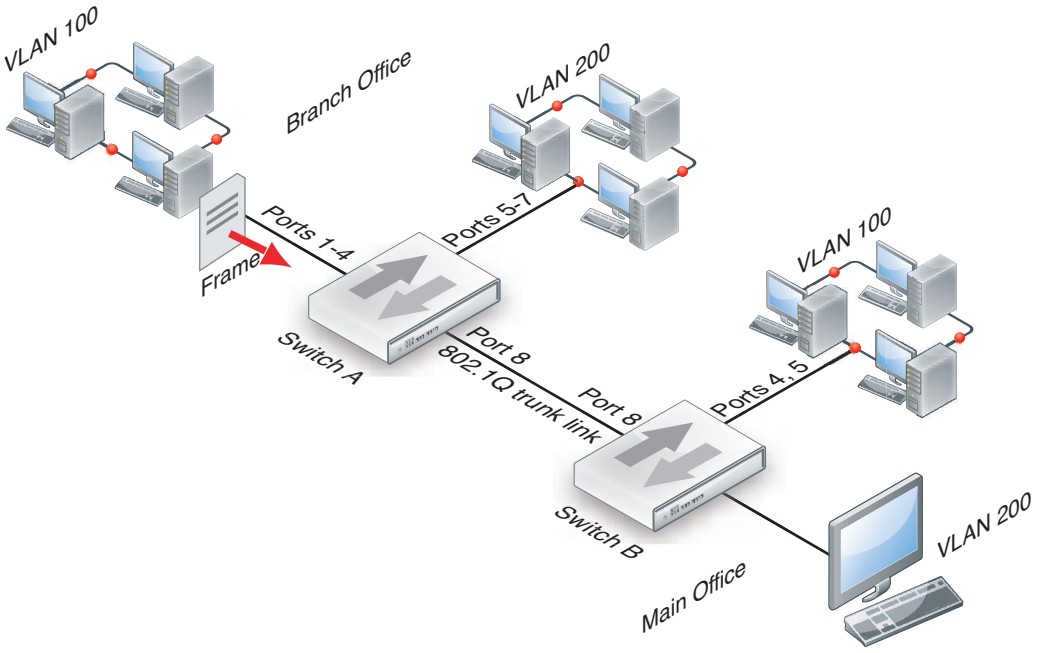
To better understand VLAN operation, this example shows what happens to a data frame on a network that uses VLANs.

The network topology consists of two 8-port switches that are configured to support VLANs on a network. Both switches are connected through port 8 using an 802.1Q trunk link. Subnet 1 is connected to switch A, and subnet 2 is connected to switch B. The ports on the switches are configured as follows.

How ports and VLANs are used on Switch A and Switch B

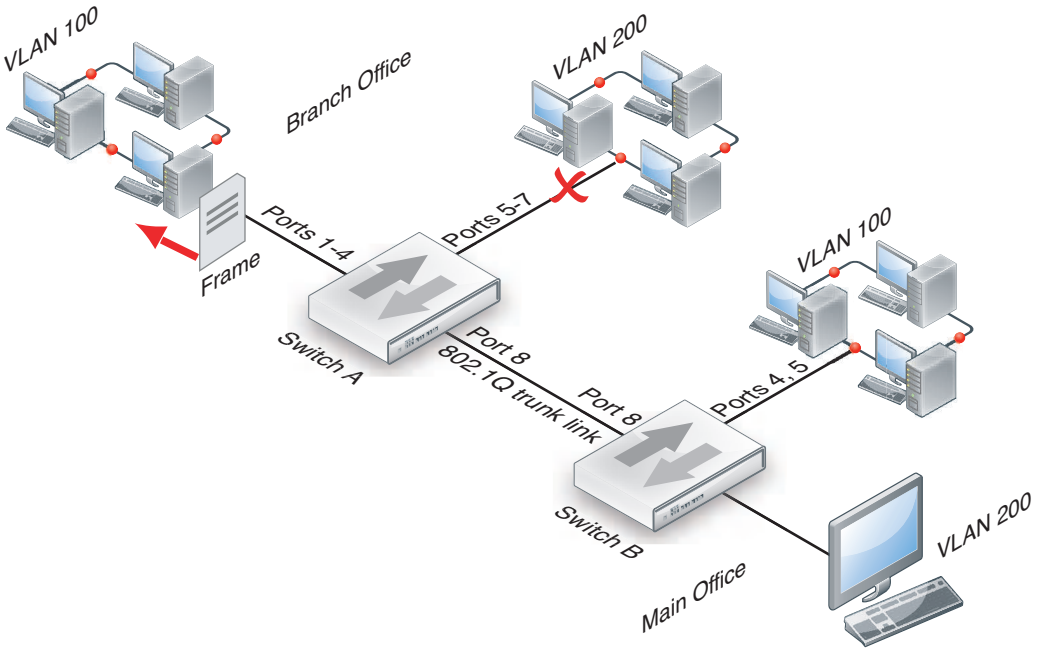
Switch	Ports	VLAN
A	1 - 4	100
A	5 - 7	200
A & B	8	Trunk link
B	4 - 5	100
B	6	200

In this example, switch A is connected to the Branch Office and switch B to the Main Office.



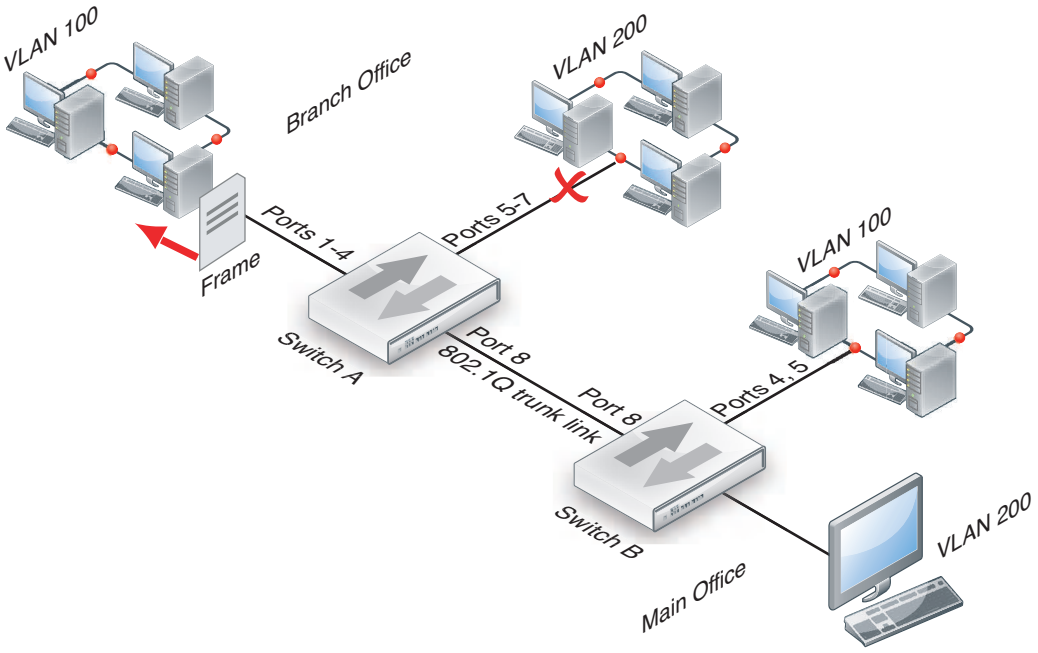
1. A computer on port 1 of switch A sends a data frame over the network.
2. Switch A tags the data frame with a VLAN 100 ID tag upon arrival because port 1 is part of VLAN 100.
3. Switch A forwards the tagged data frame to the other VLAN 100 ports — ports 2 through 4. Switch A also forwards the data frame to the 802.1Q trunk link (port 8) so other parts of the network that may contain VLAN 100 groups will receive VLAN 100 traffic.

This data frame is not forwarded to the other ports on switch A because they are not part of VLAN 100. This increases security and decreases network traffic.



4. Switch B receives the data frame over the trunk link (port 8).
5. Because there are VLAN 100 ports on switch B (ports 4 and 5), the data frame is forwarded to those ports. As with switch A, the data frame is not delivered to VLAN 200.

   If there were no VLAN 100 ports on switch B, the switch would not forward the data frame and it would stop there.



6. The switch removes the VLAN 100 ID tag before it forwards the data frame to an end destination.

The sending and receiving computers are not aware of any VLAN tagging on the data frames that are being transmitted. When any computer receives that data frame, it appears as a normal data frame.

VLAN layer-3 routing

Routers are layer-3 devices. Layer 3 refers to the third layer of the OSI networking model, the Network layer. FortiGate units in NAT mode act as layer-3 devices. As with layer 2, FortiGate units acting as layer-3 devices are 802.1Q-compliant.

The main difference between layer-2 and layer-3 devices is how they process VLAN tags. Layer-2 switches just add, read and remove the tags. They do not alter the tags or do any other high-level actions. Layer-3 routers not only add, read and remove tags but also analyze the data frame and its contents. This analysis allows layer-3 routers to change the VLAN tag if it is appropriate and send the data frame out on a different VLAN.

In a layer-3 environment, the 802.1Q-compliant router receives the data frame and assigns a VLAN ID. The router then forwards the data frame to other members of the same VLAN broadcast domain. The broadcast domain can include local ports, layer-2 devices and layer-3 devices such as routers and firewalls. When a layer-3 device receives the data frame, the device removes the VLAN tag and examines its contents to decide what to do with the data frame. The layer-3 device considers:

- Source and destination addresses
- Protocol
- Port number

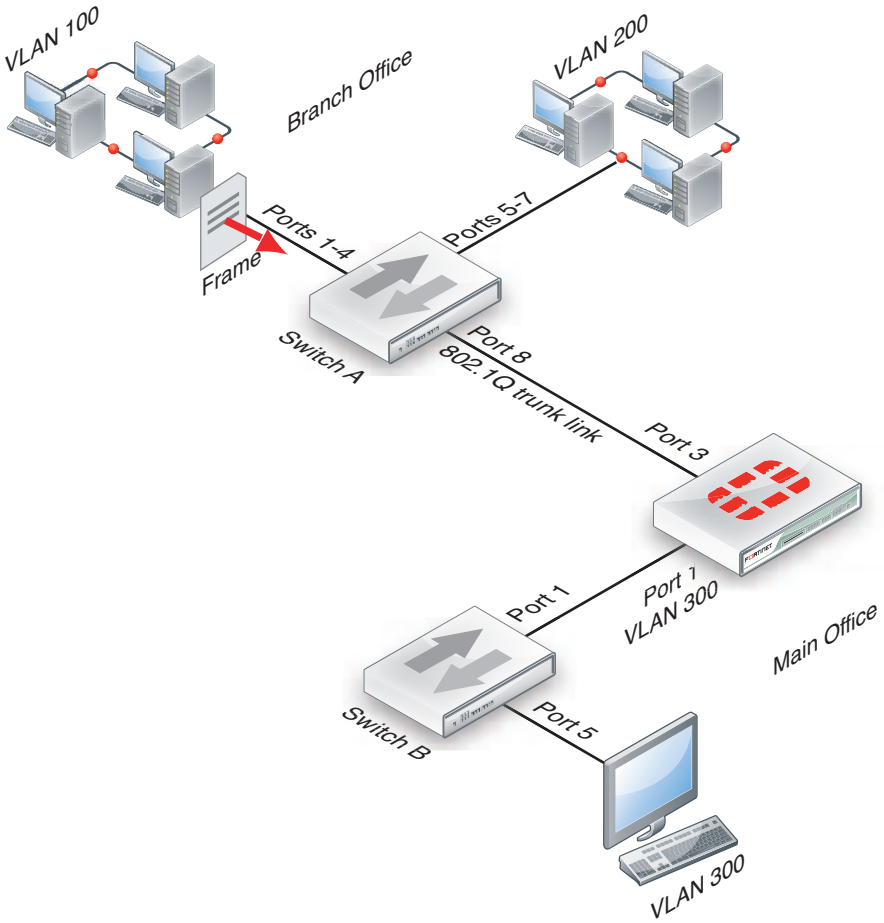
The data frame may be forwarded to another VLAN, sent to a regular non-VLAN-tagged network or just forwarded to the same VLAN as a layer-2 switch would do. Or, the data frame may be discarded if the proper security policy has been configured to do so.

Layer-3 VLAN example

In this example, switch A is connected to the Branch Office subnet, the same as subnet 1 in the layer-2 example. In the Main Office subnet, VLAN 300 is on port 5 of switch B. The FortiGate unit is connected to switch B on port 1 and the trunk link connects the FortiGate unit's port 3 to switch A. The other ports on switch B are unassigned.

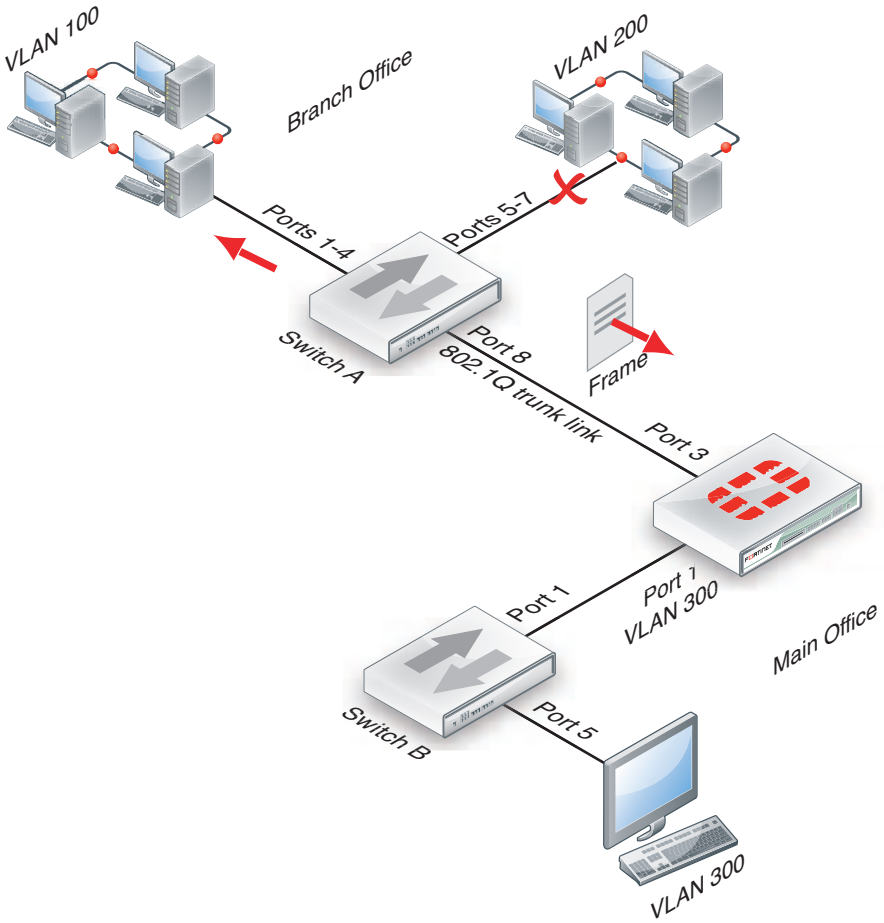
This example explains how traffic can change VLANs originating on VLAN 100 and arriving at a destination on VLAN 300. Layer-2 switches alone cannot accomplish this, but a layer-3 router can.

1. The VLAN 100 computer at the Branch Office sends the data frame to switch A, where the VLAN 100 tag is added.



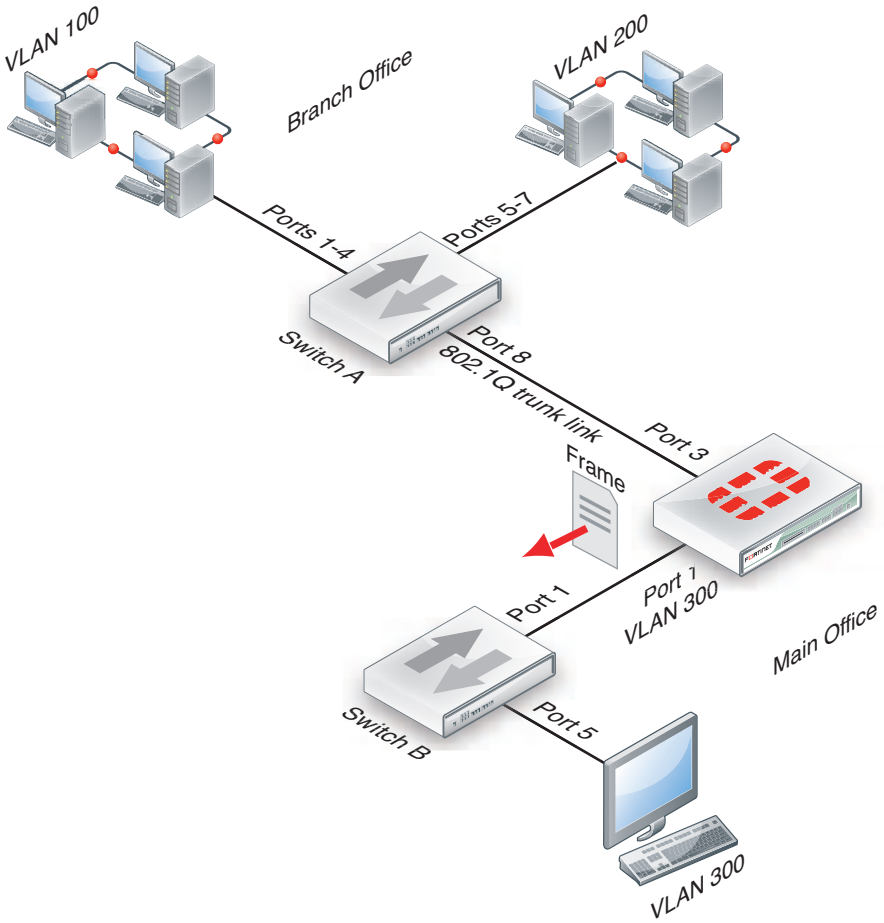
2. Switch A forwards the tagged data frame to the FortiGate unit over the 802.1Q trunk link, and to the VLAN 100 interfaces on Switch A.

   Up to this point everything is the same as in the layer-2 example.

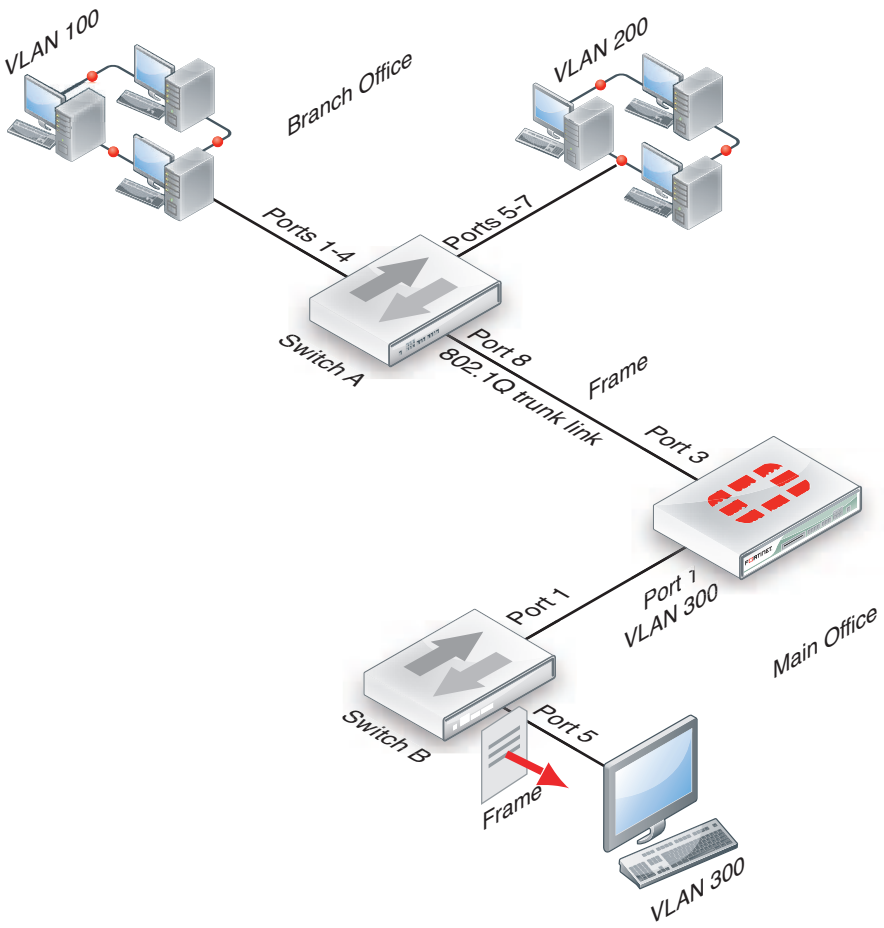


3. The FortiGate unit removes the VLAN 100 tag, and inspects the content of the data frame. The FortiGate unit uses the content to select the correct security policy and routing options.
4. The FortiGate unit's security policy allows the data frame to go to VLAN 300 in this example. The data frame will be sent to all VLAN 300 interfaces, but in the example there is only port 1 on the FortiGate unit. Before the data frame leaves, the FortiGate unit adds the VLAN ID 300 tag to the data frame.

   This is the step that layer 2 cannot do. Only layer 3 can retag a data frame as a different VLAN.



5. Switch B receives the data frame, and removes the VLAN ID 300 tag, because this is the last hop, and forwards the data frame to the computer on port 5.



In this example, a data frame arrived at the FortiGate unit tagged as VLAN 100. After checking its content, the FortiGate unit retagged the data frame for VLAN 300. It is this change from VLAN 100 to VLAN 300 that requires a layer-3 routing device, in this case the FortiGate unit. Layer-2 switches cannot perform this change.

VLANs in NAT mode

In NAT mode the FortiGate unit functions as a layer-3 device. In this mode, the FortiGate unit controls the flow of packets between VLANs, but can also remove VLAN tags from incoming VLAN packets. The FortiGate unit can also forward untagged packets to other networks, such as the Internet.

In NAT mode, the FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switches, or routers. The trunk link transports VLAN-tagged packets between physical subnets or networks. When you add VLAN sub-interfaces to the FortiGate unit physical interfaces, the VLANs have IDs that match the VLAN IDs of packets on the trunk link. The FortiGate unit directs packets with VLAN IDs to sub-interfaces with matching IDs.

You can define VLAN sub-interfaces on all FortiGate physical interfaces. However, if multiple virtual domains are configured on the FortiGate unit, you will have access to only the physical interfaces on your virtual domain. The FortiGate unit can tag packets leaving on a VLAN subinterface. It can also remove VLAN tags from incoming packets and add a different VLAN tag to outgoing packets.

Normally in VLAN configurations, the FortiGate unit's internal interface is connected to a VLAN trunk, and the external interface connects to an Internet router that is not configured for VLANs. In this configuration the

FortiGate unit can apply different policies for traffic on each VLAN interface connected to the internal interface, which results in less network traffic and better security.

Adding VLAN subinterfaces

A VLAN subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

Adding a VLAN subinterface includes configuring:

- Physical interface
- IP address and netmask
- VLAN ID
- VDOM

Physical interface

The term VLAN subinterface correctly implies the VLAN interface is not a complete interface by itself. You add a VLAN subinterface to the physical interface that receives VLAN-tagged packets. The physical interface can belong to a different VDOM than the VLAN, but it must be connected to a network router that is configured for this VLAN. Without that router, the VLAN will not be connected to the network, and VLAN traffic will not be able to access this interface. The traffic on the VLAN is separate from any other traffic on the physical interface.

When you are working with interfaces on your FortiGate unit, use the **Column Settings** on the Interface display to make sure the information you need is displayed. When working with VLANs, it is useful to position the **VLAN ID** column close to the IP address. If you are working with VDOMs, including the **Virtual Domain** column as well will help you troubleshoot problems more quickly.

To view the Interface display, go to **System > Network > Interface**.

IP address and netmask

FortiGate unit interfaces cannot have overlapping IP addresses. The IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask pair. This rule helps prevent a broadcast storm or other similar network problems.

If you are unable to change your existing configurations to prevent IP overlap, enter the CLI command `config system settings` and `set allow-subnet-overlap enable` to allow IP address overlap. If you enter this command, multiple VLAN interfaces can have an IP address that is part of a subnet used by another interface. This command is recommended for advanced users only.

VLAN ID

The VLAN ID is part of the VLAN tag added to the packets by VLAN switches and routers. The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together. VLAN ID 0 is used only for high priority frames, and 4095 is reserved.

All devices along a route must support the VLAN ID of the traffic along that route. Otherwise, the traffic will be discarded before reaching its destination. For example, if your computer is part of VLAN_100 and a co-worker on

a different floor of your building is also on the same VLAN_100, you can communicate with each other over VLAN_100, only if all the switches and routers support VLANs and are configured to pass along VLAN_100 traffic properly. Otherwise, any traffic you send your co-worker will be blocked or not delivered.

VDOM

If VDOMs are enabled, each VLAN subinterface must belong to a VDOM. This rule also applies for physical interfaces.

Interface-related CLI commands require a VDOM to be specified, regardless of whether the FortiGate unit has VDOMs enabled.

VLAN subinterfaces on separate VDOMs cannot communicate directly with each other. In this situation, the VLAN traffic must exit the FortiGate unit and re-enter the unit again, passing through firewalls in both directions. This situation is the same for physical interfaces.

A VLAN subinterface can belong to a different VDOM than the physical interface it is part of. This is because the traffic on the VLAN is handled separately from the other traffic on that interface. This is one of the main strengths of VLANs.

The following procedure will add a VLAN subinterface called `VLAN_100` to the FortiGate internal interface with a VLAN ID of 100. It will have an IP address and netmask of `172.100.1.1/255.255.255.0`, and allow HTTPS, PING, and Telnet administrative access. Note that in the CLI, you must enter "`set type vlan`" before setting the vlanid, and that the allowaccess protocols are lower case.

To add a VLAN subinterface in NAT mode - web-based manager

1. If **Current VDOM** appears at the bottom left of the screen, select **Global** from the list of VDOMs.
2. Go to **System > Network > Interface**.
3. Select **Create New** to add a VLAN subinterface.
4. Enter the following:

VLAN Name	VLAN_100
Type	VLAN
Interface	internal
VLAN ID	100
Addressing Mod	Manual
IP/Netmask	172.100.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

5. Select **OK**.

To view the new VLAN subinterface, select the expand arrow next to the parent physical interface (the internal interface). This will expand the display to show all VLAN subinterfaces on this physical interface. If there is no expand arrow displayed, there are no subinterfaces configured on that physical interface.

For each VLAN, the list displays the name of the VLAN, and, depending on column settings, its IP address, the Administrative access you selected for it, the VLAN ID number, and which VDOM it belongs to if VDOMs are enabled.

To add a VLAN subinterface in NAT mode - CLI

```
config system interface
   edit VLAN_100
      set interface internal
      set type vlan
      set vlanid 100
      set ip 172.100.1.1 255.255.255.0
      set allowaccess https ping telnet
end
```

Configuring security policies and routing

Once you have created a VLAN subinterface on the FortiGate unit, you need to configure security policies and routing for that VLAN. Without these, the FortiGate unit will not pass VLAN traffic to its intended destination. Security policies direct traffic through the FortiGate unit between interfaces. Routing directs traffic across the network.

Configuring security policies

Security policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Interfaces that communicate with the VLAN interface need security policies to permit traffic to pass between them and the VLAN interface.

Each VLAN needs a security policy for each of the following connections the VLAN will be using:

- From this VLAN to an external network
- From an external network to this VLAN
- From this VLAN to another VLAN in the same virtual domain on the FortiGate unit
- From another VLAN to this VLAN in the same virtual domain on the FortiGate unit.

The packets on each VLAN are subject to antivirus scans and other UTM measures as they pass through the FortiGate unit.

Configuring routing

As a minimum, you need to configure a default static route to a gateway with access to an external network for outbound packets. In more complex cases, you will have to configure different static or dynamic routes based on packet source and destination addresses.

As with firewalls, you need to configure routes for VLAN traffic. VLANs need routing and a gateway configured to send and receive packets outside their local subnet just as physical interfaces do. The type of routing you configure, static or dynamic, will depend on the routing used by the subnet and interfaces you are connecting to. Dynamic routing can be routing information protocol (RIP), border gateway protocol (BGP), open shortest path first (OSPF), or multicast.

If you enable SSH, PING, Telnet, HTTPS and HTTP on the VLAN, you can use those protocols to troubleshoot your routing and test that it is properly configured. Enabling logging on the interfaces and using CLI diagnose commands such as `diagnose sniff packet <interface_name>` can also help locate any possible configuration or hardware issues.

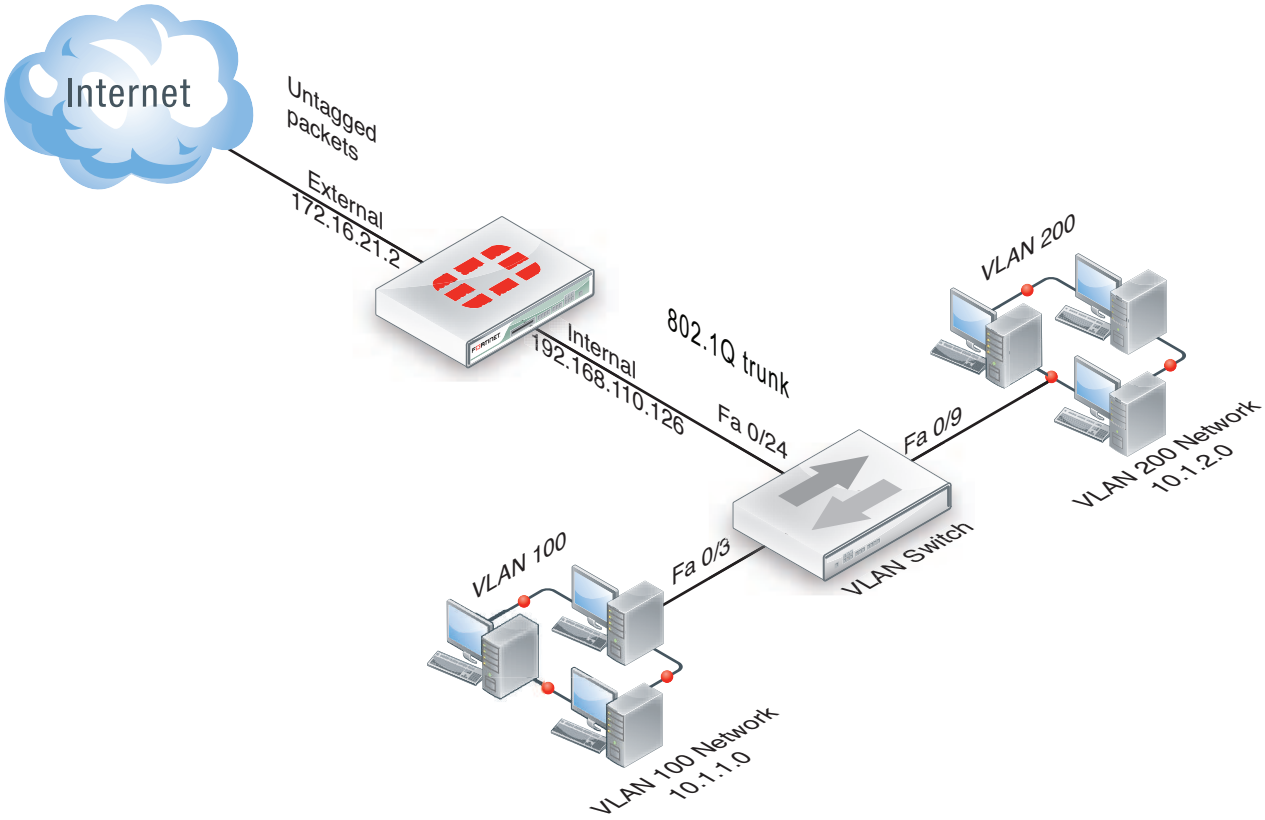
Example VLAN configuration in NAT mode

In this example two different internal VLAN networks share one interface on the FortiGate unit, and share the connection to the Internet. This example shows that two networks can have separate traffic streams while sharing a single interface. This configuration could apply to two departments in a single company, or to different companies.

There are two different internal network VLANs in this example. VLAN_100 is on the 10.1.1.0/255.255.255.0 subnet, and VLAN_200 is on the 10.1.2.0/255.255.255.0 subnet. These VLANs are connected to the VLAN switch, such as a Cisco 2950 Catalyst switch.

The FortiGate internal interface connects to the VLAN switch through an 802.1Q trunk. The internal interface has an IP address of 192.168.110.126 and is configured with two VLAN subinterfaces (VLAN_100 and VLAN_200). The external interface has an IP address of 172.16.21.2 and connects to the Internet. The external interface has no VLAN subinterfaces.

FortiGate unit with VLANs in NAT mode



When the VLAN switch receives packets from VLAN_100 and VLAN_200, it applies VLAN ID tags and forwards the packets of each VLAN both to local ports and to the FortiGate unit across the trunk link. The FortiGate unit has policies that allow traffic to flow between the VLANs, and from the VLANs to the external network.

This section describes how to configure a FortiGate unit and a Cisco Catalyst 2950 switch for this example network topology. The Cisco configuration commands used in this section are IOS commands.

It is assumed that both the FortiGate unit and the Cisco 2950 switch are installed and connected and that basic configuration has been completed. On the switch, you will need to be able to access the CLI to enter commands. Refer to the manual for your FortiGate model as well as the manual for the switch you select for more information.

It is also assumed that no VDOMs are enabled.

General configuration steps

The following steps provide an overview of configuring and testing the hardware used in this example. For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configure the FortiGate unit
   - Configure the external interface
   - Add two VLAN subinterfaces to the internal network interface
   - Add firewall addresses and address ranges for the internal and external networks
   - Add security policies to allow:
- the VLAN networks to access each other
- the VLAN networks to access the external network.
2. Configure the VLAN switch

Configure the FortiGate unit

Configuring the FortiGate unit includes:

Configure the external interface

The FortiGate unit's external interface will provide access to the Internet for all internal networks, including the two VLANs.

To configure the external interface - web-based manager

1. Go to **System > Network > Interface**.
2. Select **Edit** for the external interface.
3. Enter the following information and select **OK**:

Addressing mode	Manual
IP/Network Mask	172.16.21.2/255.255.255.0

To configure the external interface - CLI

```
config system interface
   edit external
      set mode static
      set ip 172.16.21.2 255.255.255.0
end
```

Add VLAN subinterfaces

This step creates the VLANs on the FortiGate unit internal physical interface. The IP address of the internal interface does not matter to us, as long as it does not overlap with the subnets of the VLAN subinterfaces we are configuring on it.

The rest of this example shows how to configure the VLAN behavior on the FortiGate unit, configure the switches to direct VLAN traffic the same as the FortiGate unit, and test that the configuration is correct.

Adding VLAN subinterfaces can be completed through the web-based manager, or the CLI.

To add VLAN subinterfaces - web-based manager

1. Go to **System > Network > Interface**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100
Interface	internal
VLAN ID	100
Addressing mode	Manual
IP/Network Mask	10.1.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_200
Interface	internal
VLAN ID	200
Addressing mode	Manual
IP/Network Mask	10.1.2.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

To add VLAN subinterfaces - CLI

```
config system interface
   edit VLAN_100
      set vdom root
      set interface internal
      set type vlan
      set vlanid 100
      set mode static
      set ip 10.1.1.1 255.255.255.0
```

```
      set allowaccess https ping telnet
   next
   edit VLAN_200
      set vdom root
      set interface internal
      set type vlan
      set vlanid 200
      set mode static
      set ip 10.1.2.1 255.255.255.0
      set allowaccess https ping telnet
end
```

Add the firewall addresses

You need to define the addresses of the VLAN subnets for use in security policies. The FortiGate unit provides one default address, “all”, that you can use when a security policy applies to all addresses as a source or destination of a packet. However, using “all” is less secure and should be avoided when possible.

In this example, the “_Net” part of the address name indicates a range of addresses instead of a unique address. When choosing firewall address names, use informative and unique names.

To add the firewall addresses - web-based manager

1. Go to **Firewall Objects > Address > Addresses**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100_Net
Type	Subnet
Subnet / IP Range	10.1.1.0/255.255.255.0

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_200_Net
Type	Subnet
Subnet / IP Range	10.1.2.0/255.255.255.0

To add the firewall addresses - CLI

```
config firewall address
   edit VLAN_100_Net
      set type ipmask
      set subnet 10.1.1.0 255.255.255.0
   next
   edit VLAN_200_Net
      set type ipmask
      set subnet 10.1.2.0 255.255.255.0
end
```

Add the security policies

Once you have assigned addresses to the VLANs, you need to configure security policies for them to allow valid packets to pass from one VLAN to another and to the Internet.

You can customize the Security Policy display by including some or all columns, and customize the column order onscreen. Due to this feature, security policy screenshots may not appear the same as on your screen.

If you do not want to allow all services on a VLAN, you can create a security policy for each service you want to allow. This example allows all services.

To add the security policies - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
2. Leave the **Policy Type** as **Firewall** and the **Policy Subtype** as **Address**.
3. Enter the following information and select **OK**:

Incoming Interface	VLAN_100
Source Address	VLAN_100_Net
Outgoing Interface	VLAN_200
Destination Address	VLAN_200_Net
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

4. Select **Create New**.
5. Leave the **Policy Type** as **Firewall** and the **Policy Subtype** as **Address**.
6. Enter the following information and select **OK**:

Incoming Interface	VLAN_200
Source Address	VLAN_200_Net
Outgoing Interface	VLAN_100
Destination Address	VLAN_100_Net
Schedule	Always
Service	ALL
Action	ACCEPT

Enable NAT	Enable

7. Select **Create New**.
8. Leave the **Policy Type** as **Firewall** and the **Policy Subtype** as **Address**.
9. Enter the following information and select **OK**:

Incoming Interface	VLAN_100
Source Address	VLAN_100_Net
Outgoing Interface	external
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

10. Select **Create New**.
11. Verify that the **Policy Type** is **Firewall** and the **Policy Subtype** is **Address**.
12. Enter the following information and select **OK**:

Incoming Interface	VLAN_200
Source Address	VLAN_200_Net
Outgoing Interface	external
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

To add the security policies - CLI

```
config firewall policy or Config firewall policy6
   edit 1
      set srcintf VLAN_100
      set srcaddr VLAN_100_Net
      set dstintf VLAN_200
      set dstaddr VLAN_200_Net
      set schedule always
      set service ALL
      set action accept
      set nat enable
```

```
        set status enable
    next
    edit 2
        set srcintf VLAN_200
        set srcaddr VLAN_200_Net
        set dstintf VLAN_100
        set dstaddr VLAN_100_Net
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
    next
    edit 3
        set srcintf VLAN_100
        set srcaddr VLAN_100_Net
        set dstintf external
        set dstaddr all
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
    next
    edit 4
        set srcintf VLAN_200
        set srcaddr VLAN_200_Net
        set dstintf external
        set dstaddr all
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
end
```

Configure the VLAN switch

On the Cisco Catalyst 2950 Catalyst VLAN switch, you need to define VLANs 100 and 200 in the VLAN database, and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

One method to configure a Cisco switch is to connect over a serial connection to the console port on the switch, and enter the commands at the CLI. Another method is to designate one interface on the switch as the management interface and use a web browser to connect to the switch's graphical interface. For details on connecting and configuring your Cisco switch, refer to the installation and configuration manuals for the switch.

The switch used in this example is a Cisco Catalyst 2950 switch. The commands used are IOS commands. Refer to the switch manual for help with these commands.

To configure the VLAN subinterfaces and the trunk interfaces

Add this file to the Cisco switch:

```
!
interface FastEthernet0/3
switchport access vlan 100
!
```

```
interface FastEthernet0/9
switchport access vlan 200
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

The switch has the configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

To complete the setup, configure devices on VLAN_100 and VLAN_200 with default gateways. The default gateway for VLAN_100 is the FortiGate VLAN_100 subinterface. The default gateway for VLAN_200 is the FortiGate VLAN_200 subinterface.

Test the configuration

Use diagnostic commands, such as `tracert`, to test traffic routed through the FortiGate unit and the Cisco switch.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200.

Access a command prompt on a Windows computer on the VLAN_100 network, and enter the following command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
   1 <10 ms <10 ms <10 ms 10.1.1.1
   2 <10 ms <10 ms <10 ms 10.1.2.2
Trace complete.
```

Testing traffic from VLAN_200 to the external network

In this example, a route is traced from an internal network to the external network. The route target is the external network interface of the FortiGate-800 unit.

From VLAN_200, access a command prompt and enter this command:

```
C:\>tracert 172.16.21.2
Tracing route to 172.16.21.2 over a maximum of 30 hops:
   1 <10 ms <10 ms <10 ms 10.1.2.1
   2 <10 ms <10 ms <10 ms 172.16.21.2
Trace complete.
```

VLANs in transparent mode

In transparent mode, the FortiGate unit behaves like a layer-2 bridge but can still provide services such as antivirus scanning, web filtering, spam filtering and intrusion protection to traffic. There are some limitations in transparent mode in that you cannot use SSL VPN, PPTP/L2TP VPN, DHCP server, or easily perform NAT on traffic. The limits in transparent mode apply to IEEE 802.1Q VLAN trunks passing through the unit.

VLANs and transparent mode

You can insert the FortiGate unit operating in transparent mode into the VLAN trunk without making changes to your network. In a typical configuration, the FortiGate unit internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal network VLANs. The FortiGate external interface forwards VLAN-tagged packets through another VLAN trunk to an external VLAN switch or router and on to external networks such as the Internet. You can configure the unit to apply different policies for traffic on each VLAN in the trunk.

To pass VLAN traffic through the FortiGate unit, you add two VLAN subinterfaces with the same VLAN ID, one to the internal interface and the other to the external interface. You then create a security policy to permit packets to flow from the internal VLAN interface to the external VLAN interface. If required, you create another security policy to permit packets to flow from the external VLAN interface to the internal VLAN interface. Typically in transparent mode, you do not permit packets to move between different VLANs. Network protection features, such as spam filtering, web filtering and anti-virus scanning, are applied through the UTM profiles specified in each security policy, enabling very detailed control over traffic.

When the FortiGate unit receives a VLAN-tagged packet at a physical interface, it directs the packet to the VLAN subinterface with the matching VLAN ID. The VLAN tag is removed from the packet, and the FortiGate unit then applies security policies using the same method it uses for non-VLAN packets. If the packet exits the FortiGate unit through a VLAN subinterface, the VLAN ID for that subinterface is added to the packet and the packet is sent to the corresponding physical interface.

There are two essential steps to configure your FortiGate unit to work with VLANs in transparent mode:

- Add VLAN subinterfaces
- Create security policies

You can also configure the protection profiles that manage antivirus scanning, web filtering and spam filtering. For more information on UTM profiles, see the UTM Guide.

Add VLAN subinterfaces

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch. The VLAN ID can be any number between 1 and 4094, with 0 being used only for high priority frames and 4095 being reserved. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

For this example, we are creating a VLAN called internal_v225 on the internal interface, with a VLAN ID of 225. Administrative access is enabled for HTTPS and SSH. VDOMs are not enabled.

To add VLAN subinterfaces in transparent mode - web-based manager

1. Go to **System > Network > Interface**.
2. Select **Create New**.
3. Enter the following information and select **OK**.

Name	internal_v225
Type	VLAN
Interface	internal
VLAN ID	225
Administrative Access	Enable HTTPS, and SSH. These are very secure access methods.
Comments	VLAN 225 on internal interface

The FortiGate unit adds the new subinterface to the interface that you selected.

Repeat steps 2 and 3 to add additional VLANs. You will need to change the **VLAN ID**, **Name**, and possibly **Interface** when adding additional VLANs.

To add VLAN subinterfaces in transparent mode - CLI

```
config system interface
   edit internal_v225
      set interface internal
      set vlanid 225
      set allowaccess HTTPS SSH
      set description "VLAN 225 on internal interface"
      set vdom root
end
```

Create security policies

In transparent mode, the FortiGate unit performs antivirus and antispam scanning on each VLAN's packets as they pass through the unit. You need security policies to permit packets to pass from the VLAN interface where they enter the unit to the VLAN interface where they exit the unit. If there are no security policies configured, no packets will be allowed to pass from one interface to another.

To add security policies for VLAN subinterfaces - web based manager

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New** to add firewall addresses that match the source and destination IP addresses of VLAN packets.
3. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
4. From the **Incoming Interface/Zone** list, select the VLAN interface where packets enter the unit.
5. From the **Outgoing Interface/Zone** list, select the VLAN interface where packets exit the unit.
6. Select the **Source** and **Destination Address** names that you added in step 2.
7. Select **OK**.

To add security policies for VLAN subinterfaces - CLI

```
config firewall address
   edit incoming_VLAN_address
      set associated-interface <incoming_VLAN_interface>
      set type ipmask
      set subnet <IPv4_address_mask)
```

```
    next
    edit outgoing_VLAN_address
      set associated-interface <outgoing_VLAN_interface>
      set type ipmask
      set subnet <IPv4_address_mask>
    next
  end
  config firewall policy or config firewall policy6
    edit <unused_policy_number>
      set srcintf <incoming_VLAN_interface>
      set srcaddr incoming_VLAN_address
      set destintf <outgoing_VLAN_interface>
      set destaddr outgoing_VLAN_address
      set schedule always
      set service <protocol_to_allow_on VLAN>
      set action ACCEPT
    next
  end
```

Example of VLANs in transparent mode

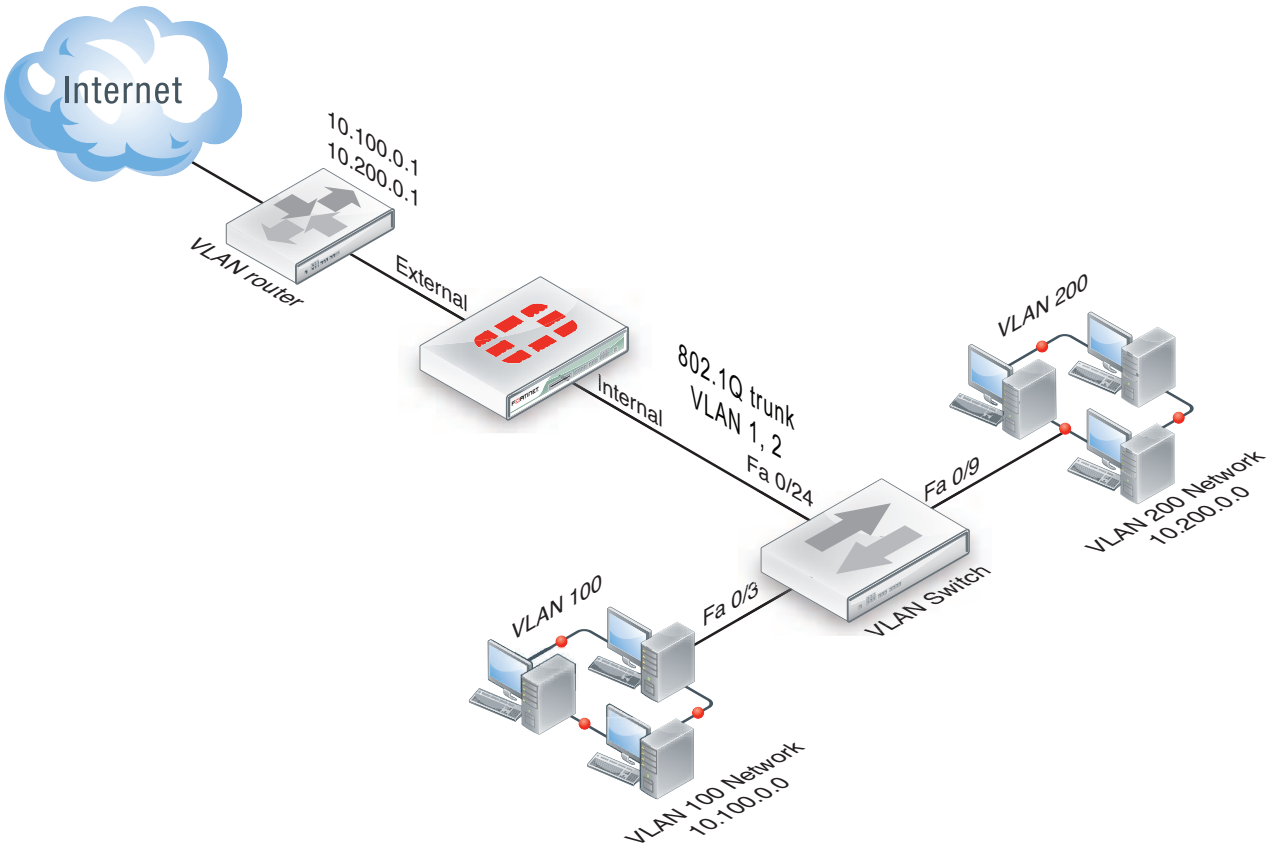
In this example, the FortiGate unit is operating in transparent mode and is configured with two VLANs: one with an ID of 100 and the other with ID 200. The internal and external physical interfaces each have two VLAN subinterfaces, one for VLAN_100 and one for VLAN_200.

The IP range for the internal VLAN_100 network is 10.100.0.0/255.255.0.0, and for the internal VLAN_200 network is 10.200.0.0/255.255.0.0.

The internal networks are connected to a Cisco 2950 VLAN switch, which combines traffic from the two VLANs onto one in the FortiGate unit internal interface. The VLAN traffic leaves the FortiGate unit on the external network interface, goes on to the VLAN switch, and on to the Internet. When the FortiGate units receives a tagged packet, it directs it from the incoming VLAN subinterface to the outgoing VLAN subinterface for that VLAN.

This section describes how to configure a FortiGate-800 unit, Cisco switch, and Cisco router in the network topology shown below.

VLAN transparent network topology



General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configure the FortiGate unit which includes
   - Adding VLAN subinterfaces
   - Adding the security policies
2. Configure the Cisco switch and router

Configure the FortiGate unit

The FortiGate unit must be configured with the VLAN subinterfaces and the proper security policies to enable traffic to flow through the FortiGate unit.

Add VLAN subinterfaces

For each VLAN, you need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager

1. Go to **System > Network > Interface**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100_int
Interface	internal
VLAN ID	100

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_100_ext
Interface	external
VLAN ID	100

6. Select **Create New**.
7. Enter the following information and select **OK**:

Name	VLAN_200_int
Interface	internal
VLAN ID	200

8. Select **Create New**.
9. Enter the following information and select **OK**:

Name	VLAN_200_ext
Interface	external
VLAN ID	200

To add VLAN subinterfaces - CLI

```
config system interface
   edit VLAN_100_int
      set status down
      set type vlan
      set interface internal
```

```
    set vlanid 100
next
edit VLAN_100_ext
    set status down
    set type vlan
    set interface external
    set vlanid 100
next
edit VLAN_200_int
    set status down
    set type vlan
    set interface internal
    set vlanid 200
next
edit VLAN_200_ext
    set status down
    set type vlan
    set interface external
    set vlanid 200
end
```

Add the security policies

Security policies allow packets to travel between the VLAN_100_int interface and the VLAN_100_ext interface. Two policies are required; one for each direction of traffic. The same is required between the VLAN_200_int interface and the VLAN_200_ext interface, for a total of four required security policies.

To add the security policies - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
2. Enter the following information and select **OK**:

Incoming Interface	VLAN_100_int
Source Address	all
Outgoing Interface	VLAN_100_ext
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

3. Select **Create New**.
4. Enter the following information and select **OK**:

Incoming Interface	VLAN_100_ext
Source Address	all

Outgoing Interface	VLAN_100_int
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

5. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
6. Enter the following information and select **OK**:

Incoming Interface	VLAN_200_int
Source Address	all
Outgoing Interface	VLAN_200_ext
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

7. Select **Create New**.
8. Enter the following information and select **OK**:

Incoming Interface	VLAN_200_ext
Source Address	all
Outgoing Interface	VLAN_200_int
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

To add the security policies - CLI

```
config firewall policy or config firewall policy6
   edit 1
      set srcintf VLAN_100_int
      set srcaddr all
      set dstintf VLAN_100_ext
      set dstaddr all
      set action accept
```

```
      set schedule always
      set service ALL
   next
   edit 2
      set srcintf VLAN_100_ext
      set srcaddr all
      set dstintf VLAN_100_int
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
   edit 3
      set srcintf VLAN_200_int
      set srcaddr all
      set dstintf VLAN_200_ext
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
   edit 4
      set srcintf VLAN_200_ext
      set srcaddr all
      set dstintf VLAN_200_int
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   end
```

Configure the Cisco switch and router

This example includes configuration for the Cisco Catalyst 2900 ethernet switch, and for the Cisco Multiservice 2620 ethernet router. If you have access to a different VLAN enabled switch or VLAN router you can use them instead, however their configuration is not included in this document.

Configure the Cisco switch

On the VLAN switch, you need to define VLAN_100 and VLAN_200 in the VLAN database and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to the Cisco switch:

```
interface FastEthernet0/3
switchport access vlan 100
!
interface FastEthernet0/9
switchport access vlan 200
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

Configure the Cisco router

You need to add a configuration file to the Cisco Multiservice 2620 ethernet router. The file defines the VLAN subinterfaces and the 802.1Q trunk interface on the router. The 802.1Q trunk is the physical interface on the router.

The IP address for each VLAN on the router is the gateway for that VLAN. For example, all devices on the internal VLAN_100 network will have 10.100.0.1 as their gateway.

Add this file to the Cisco router:

```
!
interface FastEthernet0/0
!
interface FastEthernet0/0.1
encapsulation dot1Q 100
ip address 10.100.0.1 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 200
ip address 10.200.0.1 255.255.255.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.2	VLAN ID 200
Port 0/0	802.1Q trunk

Test the configuration

Use diagnostic network commands such as traceroute (`tracert`) and ping to test traffic routed through the network.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 10.1.1.1
2 <10 ms <10 ms <10 ms 10.1.2.2
Trace complete.
```

Troubleshooting VLAN issues

Several problems can occur with your VLANs. Since VLANs are interfaces with IP addresses, they behave as interfaces and can have similar problems that you can diagnose with tools such as ping, traceroute, packet sniffing, and diag debug.

Asymmetric routing

You might discover unexpectedly that hosts on some networks are unable to reach certain other networks. This occurs when request and response packets follow different paths. If the FortiGate unit recognizes the response packets, but not the requests, it blocks the packets as invalid. Also, if the FortiGate unit recognizes the same packets repeated on multiple interfaces, it blocks the session as a potential attack.

This is asymmetric routing. By default, the FortiGate unit blocks packets or drops the session when this happens. You can configure the FortiGate unit to permit asymmetric routing by using the following CLI commands:

```
config system settings
   set asymroute enable
end
```

If VDOMs are enabled, this command is per VDOM. You must set it for each VDOM that has the problem as following:

```
config vdom
   edit <vdom_name>
      config system settings
      set asymroute enable
   end
end
```

If this solves your blocked traffic issue, you know that asymmetric routing is the cause. But allowing asymmetric routing is not the best solution, because it reduces the security of your network.

For a long-term solution, it is better to change your routing configuration or change how your FortiGate unit connects to your network.

If you enable asymmetric routing, antivirus and intrusion prevention systems will not be effective. Your FortiGate unit will be unaware of connections and treat each packet individually. It will become a stateless firewall.

Layer-2 and Arp traffic

By default, FortiGate units do not pass layer-2 traffic. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking. Another type of layer-2 traffic is ARP traffic.

You can allow these layer-2 protocols using the CLI command:

```
config system interface
   edit <name_str>
      set l2forward enable
   end
```

where `<name_str>` is the name of an interface.

If VDOMs are enabled, this command is per VDOM. You must set it for each VDOM that has the problem as following:

```
config vdom
   edit <vdom_name>
      config system interface
      edit <name_str>
      set l2forward enable
   end
end
```

If you enable layer-2 traffic, you may experience a problem if packets are allowed to repeatedly loop through the network. This repeated looping, very similar to a broadcast storm, occurs when you have more than one layer-2 path to a destination. Traffic may overflow and bring your network to a halt. You can break the loop by enabling Spanning Tree Protocol (STP) on your network's switches and routers. For more information, see "STP forwarding".

ARP traffic

Address Resolution Protocol (ARP) packets are vital to communication on a network, and ARP support is enabled on FortiGate unit interfaces by default. Normally you want ARP packets to pass through the FortiGate unit, especially if it is sitting between a client and a server or between a client and a router.

ARP traffic can cause problems, especially in transparent mode where ARP packets arriving on one interface are sent to all other interfaces including VLAN subinterfaces. Some layer-2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN. This instability can occur if the layer-2 switch does not maintain separate MAC address tables for each VLAN. Unstable switches may reset and cause network traffic to slow down considerably.

The default ARP timeout value is 5 minutes (300 seconds). So usually ARP entries are removed after 5 minutes. However, some conditions can cause arp entries to remain on the list for a longer time. This is not a configurable value. Enter the `get system arp` CLI command to view the ARP list.

Multiple VDOMs solution

By default, physical interfaces are in the root domain. If you do not configure any of your VLANs in the root VDOM, it will not matter how many interfaces are in the root VDOM.

The multiple VDOMs solution is to configure multiple VDOMs on the FortiGate unit, one for each VLAN. In this solution, you configure one inbound and one outbound VLAN interface in each VDOM. ARP packets are not forwarded between VDOMs. This configuration limits the VLANs in a VDOM and correspondingly reduces the administration needed per VDOM.

As a result of this configuration, the switches do not receive multiple ARP packets with duplicate MACs. Instead, the switches receive ARP packets with different VLAN IDs and different MACs. Your switches are stable.

However, you should **not** use the multiple VDOMs solution under any of the following conditions:

- You have more VLANs than licensed VDOMs
- You do not have enough physical interfaces

Instead, use one of two possible solutions, depending on which operation mode you are using:

- In NAT mode, you can use the `vlan forward` CLI command.
- In transparent mode, you can use the `forward-domain` CLI command. But you still need to be careful in some rare configurations.

Vlanforward solution

If you are using NAT mode, the solution is to use the `vlanforward` CLI command for the interface in question. By default, this command is enabled and will forward VLAN traffic to all VLANs on this interface. When disabled, each VLAN on this physical interface can send traffic only to the same VLAN. There is no cross-talk between VLANs, and ARP packets are forced to take one path along the network which prevents the multiple paths problem.

In the following example, `vlanforward` is disabled on port1. All VLANs configured on port1 will be separate and will not forward any traffic to each other.

```
config system interface
   edit port1
      set vlanforward disable
end
```

Forward-domain solution

If you are using transparent mode, the solution is to use the `forward-domain` CLI command. This command tags VLAN traffic as belonging to a particular collision group, and only VLANs tagged as part of that collision group receive that traffic. It is like an additional set of VLANs. By default, all interfaces and VLANs are part of forward-domain collision group 0. The many benefits of this solution include reduced administration, the need for fewer physical interfaces, and the availability of more flexible network solutions.

In the following example, forward-domain collision group 340 includes VLAN 340 traffic on port1 and untagged traffic on port 2. Forward-domain collision group 341 includes VLAN 341 traffic on port 1 and untagged traffic on port 3. All other interfaces are part of forward-domain collision group 0 by default. This configuration separates VLANs 340 and 341 from each other on port 1, and prevents the ARP packet problems from before.

Use these CLI commands:

```
config system interface
   edit port1
   next
   edit port2
      set forward_domain 340
   next
   edit port3
      set forward_domain 341
   next
   edit port1-340
      set forward_domain 340
      set interface port1
      set vlanid 340
   next
   edit port1-341
      set forward_domain 341
      set interface port1
      set vlanid 341
end
```

You may experience connection issues with layer-2 traffic, such as ping, if your network configuration has:

- Packets going through the FortiGate unit in transparent mode more than once
- More than one forwarding domain (such as incoming on one forwarding domain and outgoing on another)
- IPS and AV enabled.

Now IPS and AV is applied the first time packets go through the FortiGate unit, but not on subsequent passes. Only applying IPS and AV to this first pass fixes the network layer-2 related connection issues.

NetBIOS

Computers running Microsoft Windows operating systems that are connected through a network rely on a WINS server to resolve host names to IP addresses. The hosts communicate with the WINS server by using the NetBIOS protocol.

To support this type of network, you need to enable the forwarding of NetBIOS requests to a WINS server. The following example will forward NetBIOS requests on the internal interface for the WINS server located at an IP address of 192.168.111.222.

```
config system interface
   edit internal
      set netbios_forward enable
      set wins-ip 192.168.111.222
end
```

These commands apply only in NAT mode. If VDOMs are enabled, these commands are per VDOM. You must set them for each VDOM that has the problem.

STP forwarding

The FortiGate unit does not participate in the Spanning Tree Protocol (STP). STP is an IEEE 802.1 protocol that ensures there are no layer-2 loops on the network. Loops are created when there is more than one route for traffic to take and that traffic is broadcast back to the original switch. This loop floods the network with traffic, reducing available bandwidth to nothing.

If you use your FortiGate unit in a network topology that relies on STP for network loop protection, you need to make changes to your FortiGate configuration. Otherwise, STP recognizes your FortiGate unit as a blocked link and forwards the data to another path. By default, your FortiGate unit blocks STP as well as other non-IP protocol traffic.

Using the CLI, you can enable forwarding of STP and other layer-2 protocols through the interface. In this example, layer-2 forwarding is enabled on the external interface:

```
config system interface
   edit external
      set l2forward enable
      set stpforward enable
end
```

By substituting different commands for `stpforward enable`, you can also allow layer-2 protocols such as IPX, PPTP or L2TP to be used on the network.

Too many VLAN interfaces

Any virtual domain can have a maximum of 255 interfaces in transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. NAT mode supports from 255 to 8192 depending on the FortiGate model. This total number of interfaces includes VLANs, other virtual interfaces, and physical interfaces.

Your FortiGate unit may allow you to configure more interfaces than this. However, if you configure more than 255 interfaces, your system will become unstable and, over time, will not work properly. As all interfaces are used, they will overflow the routing table that stores the interface information, and connections will fail. When you try to add more interfaces, an error message will state that the maximum limit has already been reached.

If you see this error message, chances are you already have too many VLANs on your system and your routing has become unstable. To verify, delete a VLAN and try to add it back. If you have too many, you will not be able to add it back on to the system. In this case, you will need to remove enough interfaces (including VLANs) so that the total number of interfaces drops to 255 or less. After doing this, you should also reboot your FortiGate unit to clean up its memory and buffers, or you will continue to experience unstable behavior.

To configure more than 255 interfaces on your FortiGate unit in transparent mode, you have to configure multiple VDOMs, each with many VLANs. However, if you want to create more than the default 10 VDOMs (or a maximum of 2550 interfaces), you must buy a license for additional VDOMs.

With these extra licenses, you can configure up to 500 VDOMs, with each VDOM containing up to 255 VLANs in transparent mode. This is a theoretical maximum of over 127 500 interfaces. However, system resources will quickly get used up before reaching that theoretical maximum. To achieve the maximum number of VDOMs, you need to have top-end hardware with the most resources possible.

In NAT mode, if you have a top-end model, the maximum interfaces per VDOM can be as high as 8192, enough for all the VLANs in your configuration.

Your FortiGate unit has limited resources, such as CPU load and memory, that are divided between all configured VDOMs. When running 250 or more VDOMs, you may need to monitor the system resources to ensure there is enough to support the configured traffic processing.

PPTP and L2TP

A virtual private network (VPN) is a way to use a public network, such as the Internet, as a vehicle to provide remote offices or individual users with secure access to private networks. FortiOS supports the Point-to-Point Tunneling Protocol (PPTP), which enables interoperability between FortiGate units and Windows or Linux PPTP clients. Because FortiGate units support industry standard PPTP VPN technologies, you can configure a PPTP VPN between a FortiGate unit and most third-party PPTP VPN peers.

This section describes how to configure PPTP and L2TP VPNs as well as PPTP passthrough.

This section includes the topics:

- How PPTP VPNs work
- FortiGate unit as a PPTP server
- Configuring the FortiGate unit for PPTP VPN
- Configuring the FortiGate unit for PPTP pass through
- Testing PPTP VPN connections
- Logging VPN events
- Configuring L2TP VPNs
- L2TP configuration overview

How PPTP VPNs work

The Point-to-Point Tunneling Protocol enables you to create a VPN between a remote client and your internal network. Because it is a Microsoft Windows standard, PPTP does not require third-party software on the client computer. As long as the ISP supports PPTP on its servers, you can create a secure connection by making relatively simple configuration changes to the client computer and the FortiGate unit.

PPTP uses Point-to-Point protocol (PPP) authentication protocols so that standard PPP software can operate on tunneled PPP links. PPTP packages data in PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.

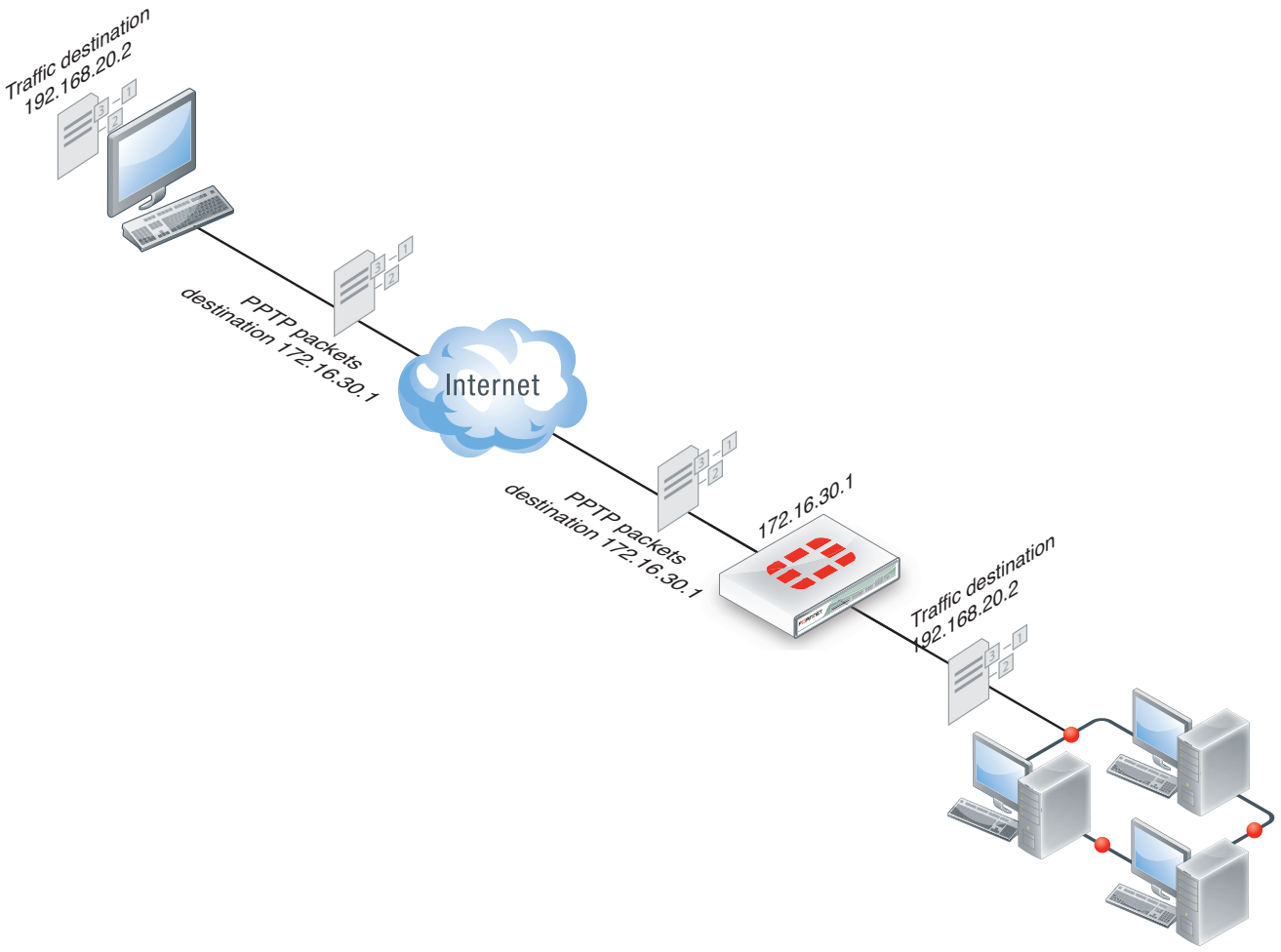
When the FortiGate unit acts as a PPTP server, a PPTP session and tunnel is created as soon as the PPTP client connects to the FortiGate unit. More than one PPTP session can be supported on the same tunnel. FortiGate units support PAP, CHAP, and plain text authentication. PPTP clients are authenticated as members of a user group.

Traffic from one PPTP peer is encrypted using PPP before it is encapsulated using Generic Routing Encapsulation (GRE) and routed to the other PPTP peer through an ISP network. PPP packets from the remote client are addressed to a computer on the private network behind the FortiGate unit. PPTP packets from the remote client are addressed to the public interface of the FortiGate unit. Seethe figure below.

PPTP control channel messages are not authenticated, and their integrity is not protected. Furthermore, encapsulated PPP packets are not cryptographically protected and may be read or modified unless appropriate encryption software such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) is used to transfer data after the tunnel has been established.

As an alternative, you can use encryption software such as Microsoft Point-to-Point Encryption (MPPE) to secure the channel. MPPE is built into Microsoft Windows clients and can be installed on Linux clients. FortiGate units support MPPE.

Packet encapsulation



Shown above, traffic from the remote client is addressed to a computer on the network behind the FortiGate unit. When the PPTP tunnel is established, packets from the remote client are encapsulated and addressed to the FortiGate unit. The FortiGate unit forwards disassembled packets to the computer on the internal network.

When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

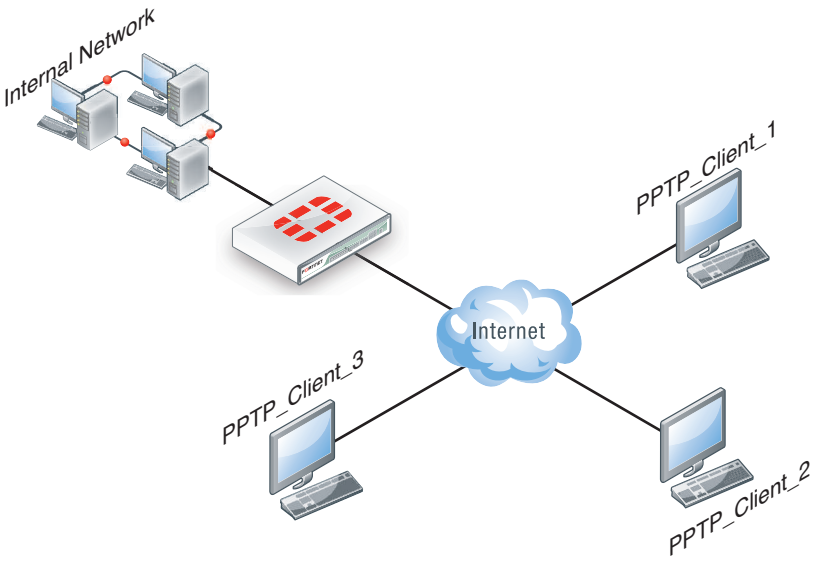
When the FortiGate unit receives a PPTP packet, the unit disassembles the PPTP packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

PPTP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate PPTP clients. All PPTP clients are challenged when a connection attempt is made.

FortiGate unit as a PPTP server

In the most common Internet scenario, the PPTP client connects to an ISP that offers PPP connections with dynamically-assigned IP addresses. The ISP forwards PPTP packets to the Internet, where they are routed to the FortiGate unit.

FortiGate unit as a PPTP server



If the FortiGate unit will act as a PPTP server, there are a number of steps to complete:

- Configure user authentication for PPTP clients.
- Enable PPTP.
- Specify the range of addresses that are assigned to PPTP clients when connecting
- Configure the security policy.

Configuring user authentication for PPTP clients

To enable authentication for PPTP clients, you must create user accounts and a user group to identify the PPTP clients that need access to the network behind the FortiGate unit. Within the user group, you must add a user for each PPTP client.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS, LDAP, or TACACS+ server. If password protection will be provided through a RADIUS, LDAP, or

TACACS+ server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

This example creates a basic user/password combination.

Configuring a user account

To add a local user - web-based manager

1. Go to **User & Device > User > User Definition** and select **Create New.**
2. Select **Local User**
3. Enter a **User Name**.
4. Enter a **Password** for the user. The password should be at least six characters.
5. Select **OK**.

To add a local user - CLI

```
config user local
   edit <username>
      set type password
      set passwd <password>
end
```

Configuring a user group

To ease configuration, create user groups that contain users in similar categories or departments.

To create a user group - web-based manager

1. Go to **User & Device > User > User Group** and select **Create New**.
2. Enter a **Name** for the group.
3. Select the **Type** of **Firewall**.
4. From the **Available Users** list, select the required users and select the right-facing arrow to add them to the **Members** list.
5. Select **OK**.

To create a user group - CLI

```
config user group
   edit <group_name>
      set group-type firewall
      set member <user_names>
end
```

Enabling PPTP and specifying the PPTP IP address range

The PPTP address range specifies the range of addresses reserved for remote PPTP clients. When a PPTP client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the PPTP client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the PPTP client appear to be part of the internal network.

PPTP requires two IP addresses, one for each end of the tunnel. The PPTP address range is the range of addresses reserved for remote PPTP clients. When the remote PPTP client establishes a connection, the FortiGate unit assigns an IP address from the reserved range of IP addresses to the client PPTP interface or retrieves the assigned IP address from the PPTP user group. If you use the PPTP user group, you must also define the FortiGate end of the tunnel by entering the IP address of the unit in **Local IP** (web-based manager) ***or*** `local-ip` (CLI). The PPTP client uses the assigned IP address as its source address for the duration of the connection.

PPTP configuration is only available through the CLI. In the example below, PPTP is enabled with the use of an IP range of `182.168.1.1` to `192.168.1.10` for addressing and the user group is hr_staff.

The start and end IPs in the PPTP address range must be in the same 24-bit subnet, for example, 192.168.1.1 - 192.168.1.254.

```
config vpn pptp
   set status enable
   set ip-mode range
   set eip 192.168.1.10
   set sip 192.168.1.1
   set usrgrp hr_staff
end
```

In this example, PPTP is enabled with the use of a user group for addressing, where the IP address of the PPTP server is `192.168.1.2` and the user group is `hr_admin`.

```
config vpn pptp
   set status enable
   set ip-mode range
   set local-ip 192.168.2.1
   set usrgrp hr_admin
end
```

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the PPTP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To configure the firewall for the PPTP tunnel - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
2. Complete the following and select **OK**:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the name that corresponds to the range of addresses that you reserved for PPTP clients.

Outgoing Interface	The FortiGate interface connected to the internal network.
Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit.
Schedule	always
Service	ALL
Action	ACCEPT

To configure the firewall for the PPTP tunnel - CLI

```
config firewall policy or config firewall policy6
   edit 1
      set srcintf <interface to internet>
      set dstintf <interface to internal network>
      set srcaddr <reserved_range>
      set dstaddr <internal_addresses>
      set action accept
      set schedule always
      set service ALL
end
```

Configuring the FortiGate unit for PPTP VPN

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server, perform the following tasks in the order given:

- Configure user authentication for PPTP clients.
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect.
- Configure PPTP pass through on the FortiGate unit.

Configuring the FortiGate unit for PPTP pass through

To forward PPTP packets to a PPTP server on the network behind the FortiGate unit, you need to perform the following configuration tasks on the FortiGate unit:

- Define a virtual IP address that points to the PPTP server.
- Create a security policy that allows incoming PPTP packets to pass through to the PPTP server.

The address range is the external (public) ip address range which requires access to the internal PPTP server through the FortiGate virtual port-forwarding firewall.

IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

Configuring a virtual IP address

The virtual IP address will be the address of the PPTP server host.

To define a virtual IP for PPTP pass through - web-based manager

1. Go to **Policy & Objects > Objects > Virtual IPs**.
2. Select **Create New**.
3. Choose the **VIP Type**.
4. Enter the name of the VIP, for example, `PPTP_Server`.
5. Select the **External Interface** where the packets will be received for the PPTP server.
6. Enter the **External IP Address** for the VIP.
7. Select **Port Forwarding**.
8. Set the **Protocol to TCP**.
9. Enter the **External Service Port** of `1723`, the default for PPTP.
10. Enter the **Map to Port** to `1723`.
11. Select **OK**.

To define a virtual IP for PPTP pass through - web-based manager

```
config firewall vip or config firewall vip6
   edit PPTP_Server
      set extintf <interface>
      set extip <ip_address>
      set portforward enable
      set protocol tcp
      set extport 1723
      set mappedport 1723
      set mappedip <destination IP address range>
      end
```

You can also use `config firewall vip46` to define a virtual IP from an IPv4 address to an IPv6 address or `config firewall vip64` to define a virtual IP from an IPv6 address to an IPv4 address.

Configuring a port-forwarding security policy

To create a port-forwarding security policy for PPTP pass through you must first create an address range reserved for the PPTP clients.

To create an address range - web-based manager

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Select a **Category**.
3. Enter a **Name** for the range, for example, `External_PPTP`.
4. Select a **Type** of **Subnet/IP Range**.
5. Enter the IP address range.
6. Select the **Interface** to the Internet.
7. Select **OK**.

To create an address range - CLI

```
config firewall address OR config firewall address6
   edit External_PPTP
      set type iprange
```

```
        set start-ip <ip_address>
        set end-ip <ip_address>
        set associated-interface <internet_interface>
end
```

With the address set, you can add the security policy.

To add the security policy - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
2. Complete the following and select **OK**:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the address range created in the previous step.
Outgoing Interface	The FortiGate interface connected to the PPTP server.
Destination Address	Select the VIP address created in the previous steps.
Schedule	always
Service	PPTP
Action	ACCEPT

To add the security policy - CLI

```
config firewall policy or config firewall policy6
   edit <policy_number>
      set srcintf <interface to internet>
      set dstintf <interface to PPTP server>
      set srcaddr <address_range>
      set dstaddr <PPTP_server_address>
      set action accept
      set schedule always
      set service PPTP
end
```

Testing PPTP VPN connections

To confirm that a PPTP VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The PPTP VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

PPTP VPN, activity is logged when enabling VPN logging. The FortiGate unit connection events and tunnel status (up/down) are logged.

To log VPN events

1. Go to **Log & Report > Log Config > Log Settings**.
2. Enable the storage of log messages to one or more locations.

3. Select **VPN activity event**.
4. Select **Apply**.

To view event logs

1. Go to **Log & Report > Event Log > VPN**.
2. If the option is available from the Log Type list, select the log file from disk or memory.

Configuring L2TP VPNs

This section describes how to configure a FortiGate unit to establish a Layer Two Tunneling Protocol (L2TP) tunnel with a remote dialup client. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly.

According to RFC 2661, an Access Concentrator (LAC) can establish an L2TP tunnel with an L2TP Network Server (LNS). In a typical scenario, the LAC is managed by an ISP and located on the ISP premises; the LNS is the gateway to a private network. When a remote dialup client connects to the Internet through the ISP, the ISP uses a local database to establish the identity of the caller and determine whether the caller needs access to an LNS through an L2TP tunnel. If the services registered to the caller indicate that an L2TP connection to the LNS is required, the ISP LAC attempts to establish an L2TP tunnel with the LNS.

A FortiGate unit can be configured to act as an LNS. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly, bypassing any LAC managed by an ISP. The ISP must configure its network access server to forward L2TP traffic from the remote client to the FortiGate unit directly whenever the remote client requires an L2TP connection to the FortiGate unit.

When the FortiGate unit acts as an LNS, an L2TP session and tunnel is created as soon as the remote client connects to the FortiGate unit. The FortiGate unit assigns an IP address to the client from a reserved range of IP addresses. The remote client uses the assigned IP address as its source address for the duration of the connection.

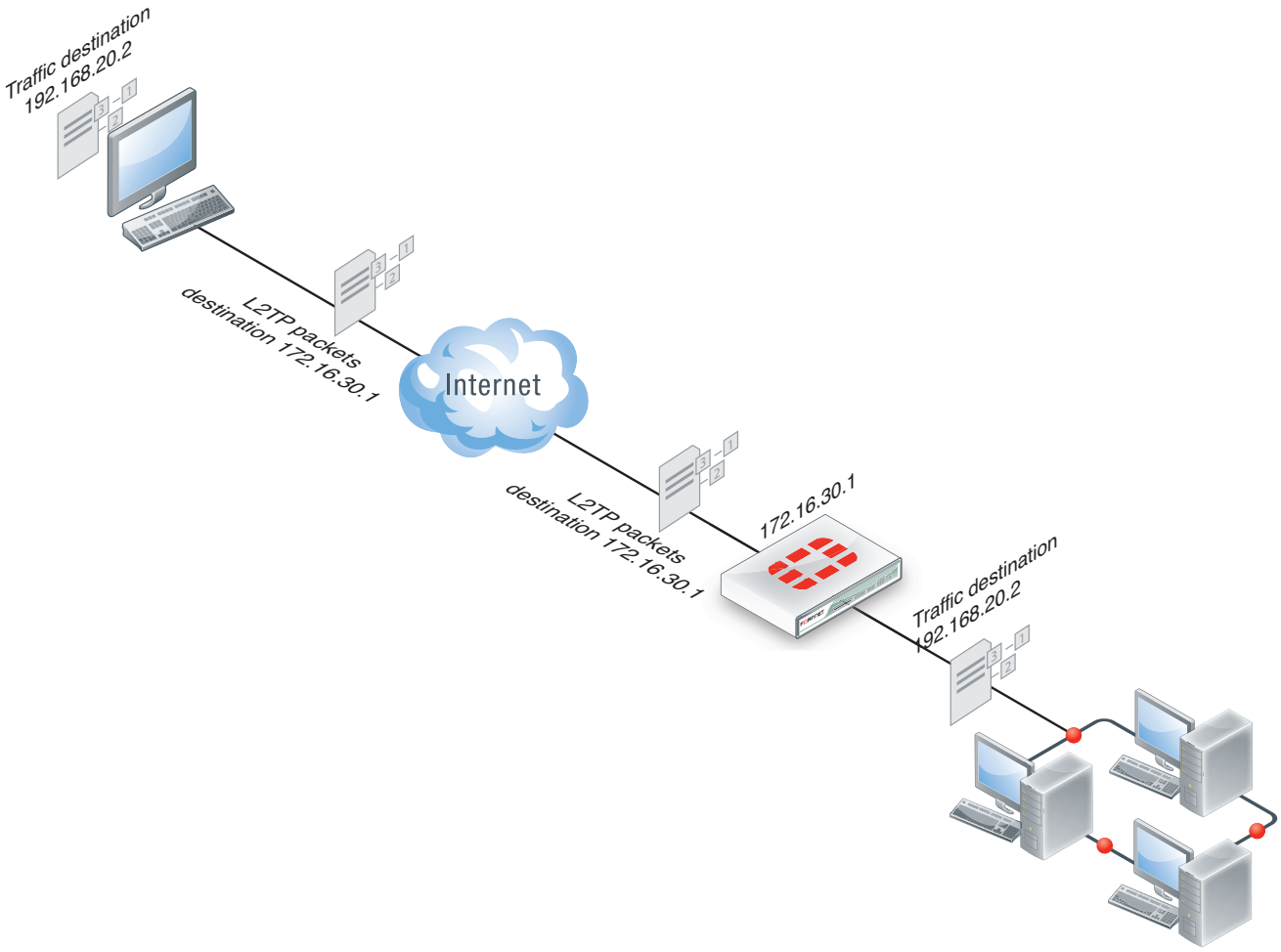
More than one L2TP session can be supported on the same tunnel. FortiGate units can be configured to authenticate remote clients using a plain text user name and password, or authentication can be forwarded to an external RADIUS or LDAP server. L2TP clients are authenticated as members of a user group.

For site-to-site connections, Windows servers use IPsec encryption when you configure the VPN to connect to an L2TP server.

Traffic from the remote client must be encrypted using IPsec before it is encapsulated and routed to the FortiGate unit. Packets originating at the remote client are addressed to a computer on the private network behind the FortiGate unit. Encapsulated packets are addressed to the public interface of the FortiGate unit. See the figure below.

When the FortiGate unit receives an L2TP packet, the unit disassembles the packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

L2TP encapsulation

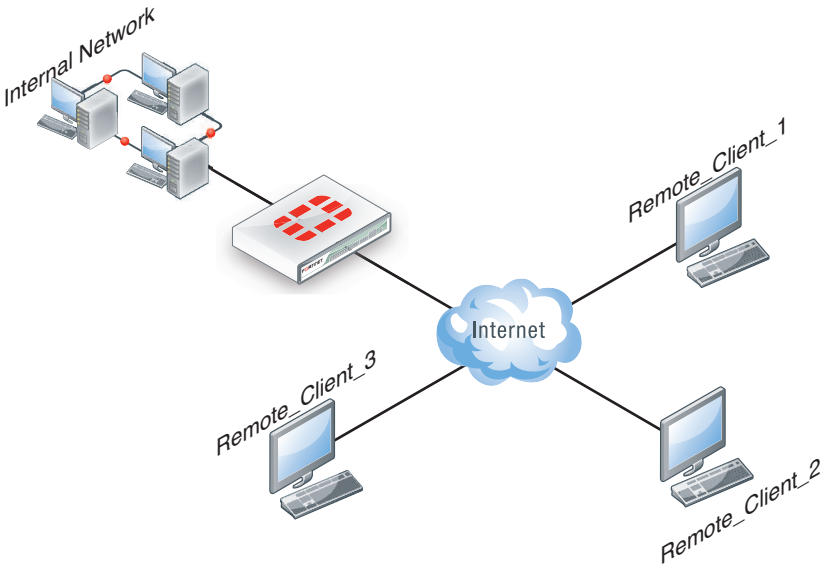


FortiGate units cannot deliver non-IP traffic such as Frame Relay or ATM frames encapsulated in L2TP packets — FortiGate units support the IPv4 and IPv6 addressing schemes only

Network topology

The remote client connects to an ISP that determines whether the client requires an L2TP connection to the FortiGate unit. If an L2TP connection is required, the connection request is forwarded to the FortiGate unit directly.

Example L2TP configuration



L2TP infrastructure requirements

- The FortiGate unit must be operating in NAT mode and have a static public IP address.
- The ISP must configure its network access server to forward L2TP traffic from remote clients to the FortiGate unit directly.
- The remote client must not generate non-IP traffic (Frame Relay or ATM frames).

L2TP configuration overview

To configure a FortiGate unit to act as an LNS, you perform the following tasks:

- Create an L2TP user group containing one user for each remote client.
- Enable L2TP on the FortiGate unit and specify the range of addresses that can be assigned to remote clients when they connect.
- Define firewall source and destination addresses to indicate where packets transported through the L2TP tunnel will originate and be delivered.
- Create the security policy and define the scope of permitted services between the source and destination addresses.
- Configure the remote clients.

Authenticating L2TP clients

L2TP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate L2TP clients. All L2TP clients are challenged when a connection attempt is made.

To enable authentication, you must create user accounts and a user group to identify the L2TP clients that need access to the network behind the FortiGate unit.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

Enabling L2TP and specifying an address range

The L2TP address range specifies the range of addresses reserved for remote clients. When a remote client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the remote client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the remote client appear to be part of the internal network.

To enable L2TP and specify the L2TP address range, use the `config vpn l2tp` CLI command.

The following example shows how to enable L2TP and set the L2TP address range using a starting address of `192.168.10.80` and an ending address of `192.168.10.100` for an existing group of L2TP users named `L2TP_users`:

```
config vpn l2tp
   set sip 192.168.10.80
   set eip 192.168.10.100
   set status enable
   set usrgrp L2TP_users
end
```

Defining firewall source and destination addresses

Before you define the security policy, you must define the source and destination addresses of packets that are to be transported through the L2TP tunnel:

- For the source address, enter the range of addresses that you reserved for remote L2TP clients (for example `192.168.10.[80-100]`).
- For the destination address, enter the IP addresses of the computers that the L2TP clients need to access on the private network behind the FortiGate unit (for example, `172.16.5.0/24` for a subnet, or `172.16.5.1` for a server or host, or `192.168.10.[10-15]` for an IP address range).

To define the firewall source address

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Select a **Category**.
3. In the **Address Name** field, type a name that represents the range of addresses that you reserved for remote clients (for example, `Ext_L2TPrange`).
4. In **Type**, select **IP Range**.
5. In the **IP Range** field, type the corresponding IP address range.
6. In **Interface**, select the FortiGate interface that connects to the clients.
7. This is usually the interface that connects to the Internet.
8. Select **OK**.

To define the firewall destination address

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. In the **Address Name** field, type a name that represents a range of IP addresses on the network behind the FortiGate unit (for example, `Int_L2TPaccess`).
3. In **Type**, select **IP Range**.
4. In the **IP Range** field, type the corresponding IP address range.
5. In **Interface**, select the FortiGate interface that connects to the network behind the FortiGate unit.
6. Select **OK**.

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the L2TP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To define the traffic and services permitted inside the L2TP tunnel

1. Go to **Policy & Objects > Policy > IPv4** or **Policy & Objects > Policy > IPv6** and select **Create New**.
2. Enter these settings:

Incoming Interface	Select the FortiGate interface to the Internet.
Source Address	Select the name that corresponds to the address range that reserved for L2TP clients (for example, `Ext_L2TPrange`).
Outgoing Interface	Select the FortiGate interface to the internal (private) network.
Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, `Int_L2TPaccess`).
Service	Select ALL, or if selected services are required instead, select the service group that you defined previously.
Action	ACCEPT

3. Select **OK**.

Configuring a Linux client

This procedure outlines how to install L2TP client software and run an L2TP tunnel on a Linux computer. Obtain an L2TP client package that meets your requirements (for example, `rp-l2tp`). If needed to encrypt traffic, obtain L2TP client software that supports encryption using IPsec.

To establish an L2TP tunnel with a FortiGate unit that has been set up to accept L2TP connections, you can obtain and install the client software following these guidelines:

1. If encryption is required, you will need to verify the IPsec configuration.
2. Download and install the L2TP client package.
3. Configure an L2TP connection to run the L2TP program.

4. Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the L2TP link and a host route to the FortiGate unit.
5. Run `l2tpd` to start the tunnel.

Follow the software supplier's documentation to complete the steps.

To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate L2TP clients. Contact the FortiGate administrator if required to obtain this information.

Monitoring L2TP sessions

You can display a list of all active sessions and view activity by port number. By default, port 1701 is used for L2TP VPN-related communications. If required, active sessions can be stopped from this view. Use the Top Sessions Dashboard Widget.

Testing L2TP VPN connections

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging L2TP VPN events

You can configure the FortiGate unit to log VPN events. For L2TP VPNs, connection events and tunnel status (up/down) are logged.

To log VPN events - web-based manager

1. Go to **Log & Report > Log Config > Log Settings**.
2. Enable the storage of log messages to one or more locations.
3. Select **Enable**, and then select **VPN activity event**.
4. Select **Apply**.

To log VPN events - CLI

```
config log memory setting
   set diskfull overwrite
   set status enable
end
config log eventfilter
   set vpn enable
end
```

Session helpers

The FortiOS firewall can analyze most TCP/IP protocol traffic by comparing packet header information to security policies. This comparison determines whether to accept or deny the packet and the session that the packet belongs to.

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. But the packets that carry the actual conversation can use a variety of UDP protocols with a variety of source and destination port numbers. The information about the protocols and port numbers used for a SIP call is contained in the body of the SIP TCP control packets. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall.

This section includes the topics:

- Viewing the session helper configuration
- Changing the session helper configuration
- DCE-RPC session helper (dcerpc)
- DNS session helpers (dns-tcp and dns-udp)
- File transfer protocol (FTP) session helper (ftp)
- H.245 session helpers (h245I and h245O)
- H.323 and RAS session helpers (h323 and ras)
- Media Gateway Controller Protocol (MGCP) session helper (mgcp)
- ONC-RPC portmapper session helper (pmap)
- PPTP session helper for PPTP traffic (pptp)
- Remote shell session helper (rsh)
- Real-Time Streaming Protocol (RTSP) session helper (rtsp)
- Session Initiation Protocol (SIP) session helper (sip)
- Trivial File Transfer Protocol (TFTP) session helper (tftp)
- Oracle TNS listener session helper (tns)

Viewing the session helper configuration

You can view the session helpers enabled on your FortiGate unit in the CLI using the commands below. The following output shows the first two session helpers. The number of session helpers can vary to around 20.

```
show system session-helper
   config system session-helper
      edit 1
         set name pptp
         set port 1723
         set protocol 6
         next
         set name h323
```

```
        set port 1720
        set protocol 6
        end
    .
    .
```

The configuration for each session helper includes the name of the session helper and the port and protocol number on which the session helper listens for sessions. Session helpers listed on protocol number 6 (TCP) or 17 (UDP). For a complete list of protocol numbers see Assigned Internet Protocol Numbers.

For example, the output above shows that FortiOS listens for PPTP packets on TCP port 1723 and H.323 packets on port TCP port 1720.

If a session helper listens on more than one port or protocol the more than one entry for the session helper appears in the `config system session-helper` list. For example, the pmap session helper appears twice because it listens on TCP port 111 and UDP port 111. The rsh session helper appears twice because it listens on TCP ports 514 and 512.

Changing the session helper configuration

Normally you will not need to change the configuration of the session helpers. However in some cases you may need to change the protocol or port the session helper listens on.

Changing the protocol or port that a session helper listens on

Most session helpers are configured to listen for their sessions on the port and protocol that they typically use. If your FortiGate unit receives sessions that should be handled by a session helper on a non-standard port or protocol you can use the following procedure to change the port and protocol used by a session helper. The following example shows how to change the port that the pmap session helper listens on for Sun RPC portmapper TCP sessions. By default pmap listens on TCP port 111.

To change the port that the pmap session helper listens on to TCP port 112

1. Confirm that the TCP pmap session helper entry is 11 in the session-helper list:

```
show system session-helper 11
    config system session-helper
        edit 11
            set name pmap
            set port 111
            set protocol 6
        next
    end
```

2. Enter the following command to change the TCP port to 112.

```
config system session-helper
    edit 11
        set port 112
        end
```

3. The pmap session helper also listens on UDP port 111. Confirm that the UDP pmap session helper entry is 12 in the session-helper list:

```
show system session-helper 12
    config system session-helper
        edit 12
```

```
            set name pmap
            set port 111
            set protocol 17
            end
```

4. Enter the following command to change the UDP port to 112.

```
config system session-helper
   edit 12
      set port 112
      end
```

Use the following command to set the h323 session helper to listen for ports on the UDP protocol.

To change the protocol that the h323 session helper listens on

1. Confirm that the h323 session helper entry is 2 in the session-helper list:

```
show system session-helper 2
   config system session-helper
      edit 2
         set name h323
         set port 1720
         set protocol 6
      next
   end
```

2. Enter the following command to change the protocol to UDP.

```
config system session-helper
   edit 2
      set protocol 17
   end
end
```

If a session helper listens on more than one port or protocol, then multiple entries for the session helper must be added to the session helper list, one for each port and protocol combination. For example, the rtsp session helper listens on TCP ports 554, 7070, and 8554 so there are three rtsp entries in the session-helper list. If your FortiGate unit receives rtsp packets on a different TCP port (for example, 6677) you can use the following command to configure the rtsp session helper to listen on TCP port 6677.

To configure a session helper to listen on a new port and protocol

```
config system session-helper
   edit 0
      set name rtsp
      set port 6677
      set protocol 6
end
```

Disabling a session helper

In some cases you may need to disable a session helper. Disabling a session helper just means removing it from the session-helper list so that the session helper is not listening on a port. You can completely disable a session helper by deleting all of its entries from the session helper list. If there are multiple entries for a session helper on the list you can delete one of the entries to prevent the session helper from listening on that port.

To disable the mgcp session helper from listening on UDP port 2427

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2427:

```
show system session-helper
   .
   .
   .
edit 19
   set name mgcp
   set port 2427
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 19 to disable the mgcp session helper from listening on UDP port 2427:

```
config system session-helper
   delete 19
```

By default the mgcp session helper listens on UDP ports 2427 and 2727. The previous procedure shows how to disable the mgcp protocol from listening on port 2427. The following procedure completely disables the mgcp session helper by also disabling it from listening on UDP port 2727.

To completely disable the mgcp session helper

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2727:

```
show system session-helper
   .
   .
   .
edit 20
   set name mgcp
   set port 2727
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 20 to disable the mgcp session helper from listening on UDP port 2727:

```
config system session-helper
   delete 20
```

DCE-RPC session helper (dcerpc)

Distributed Computing Environment Remote Procedure Call (DCE-RPC) provides a way for a program running on one host to call procedures in a program running on another host. DCE-RPC (also called MS RPC for Microsoft RPC) is similar to ONC-RPC. Because of the large number of RPC services, for example, MAPI, the transport address of an RPC service is dynamically negotiated based on the service program's universal unique identifier (UUID). The Endpoint Mapper (EPM) binding protocol in FortiOS maps the specific UUID to a transport address.

To accept DCE-RPC sessions you must add a security policy with service set to any or to the DEC-RPC pre-defined service (which listens on TCP and UDP ports 135). The dcerpc session helper also listens on TCP and UDP ports 135.

The session allows FortiOS to handle DCE-RPC dynamic transport address negotiation and to ensure UUID-based security policy enforcement. You can define a security policy to permit all RPC requests or to permit by specific UUID number.

In addition, because a TCP segment in a DCE-RPC stream might be fragmented, it might not include an intact RPC PDU. This fragmentation occurs in the RPC layer; so FortiOS does not support parsing fragmented packets.

DNS session helpers (dns-tcp and dns-udp)

FortiOS includes two DNS session helpers, dns-tcp, a session helper for DNS over TCP, and dns-udp, a session helper for DNS over UDP.

To accept DNS sessions you must add a security policy with service set to any or to the DNS pre-defined service (which listens on TCP and UDP ports 53). The dns-udp session helper also listens on UDP port 53. By default the dns-tcp session helper is disabled. If needed you can use the following command to enable the dns-tcp session helper to listen for DNS sessions on TCP port 53:

```
config system session-helper
   edit 0
      set name dns-tcp
      set port 53
      set protocol 6
end
```

File transfer protocol (FTP) session helper (ftp)

The FTP session helper monitors PORT, PASV and 227 commands and NATs the IP addresses and port numbers in the body of the FTP packets and opens ports on the FortiGate unit as required.

To accept FTP sessions you must add a security policy with service set to any or to the FTP, FTP_Put, and FTP_GET pre-defined services (which all listen on TCP port 21).

H.245 session helpers (h245I and h245O)

H.245 is a control channel protocol used for H.323 and other similar communication sessions. H.245 sessions transmit non-telephone signals. H.245 sessions carry information needed for multimedia communication, such as encryption, flow control jitter management and others.

FortiOS includes two H.245 sessions helpers, h245I which is for H.245 call in and h245O which is for H.245 call out sessions. There is no standard port for H.245. By default the H.245 sessions helpers are disabled. You can enable them as you would any other session helper. When you enable them, you should specify the port and protocol on which the FortiGate unit receives H.245 sessions.

H.323 and RAS session helpers (h323 and ras)

The H.323 session helper supports secure H.323 voice over IP (VoIP) sessions between terminal endpoints such as IP phones and multimedia devices. In H.323 VoIP networks, gatekeeper devices manage call registration, admission, and call status for VoIP calls. The FortiOS h323 session helper supports gatekeepers installed on two different networks or on the same network.

To accept H.323 sessions you must add a security policy with service set to any or to the H323 pre-defined service (which listens on TCP port numbers 1720 and 1503 and on UDP port number 1719). The h323 session helper listens on TCP port 1720.

The ras session helper is used with the h323 session helper for H.323 Registration, Admission, and Status (RAS) services. The ras session helper listens on UDP port 1719.

Alternate H.323 gatekeepers

The h323 session helper supports using H.323 alternate gatekeepers. All the H.323 end points must register with a gatekeeper through the Registration, Admission, and Status (RAS) protocol before they make calls. During the registration process, the primary gatekeeper sends Gatekeeper Confirm (GCF) and Registration Confirm (RCF) messages to the H.323 end points that contain the list of available alternate gatekeepers.

The alternate gatekeeper provides redundancy and scalability for the H.323 end points. If the primary gatekeeper fails the H.323 end points that have registered with that gatekeeper are automatically registered with the alternate gatekeeper. To use the H.323 alternate gatekeeper, you need to configure security policies that allow H.323 end points to reach the alternate gatekeeper.

Media Gateway Controller Protocol (MGCP) session helper (mgcp)

The Media Gateway Control Protocol (MGCP) is a text-based application layer protocol used for VoIP call setup and control. MGCP uses a master-slave call control architecture in which the media gateway controller uses a call agent to maintain call control intelligence, while the media gateways perform the instructions of the call agent.

To accept MGCP sessions you must add a security policy with service set to any or to the MGCP pre-defined service (which listens on UDP port numbers 2427 and 2727). The h323 session helper also listens on UDP port numbers 2427 and 2727.

The MGCP session helper does the following:

- VoIP signalling payload inspection. The payload of the incoming VoIP signalling packet is inspected and malformed packets are blocked.
- Signaling packet body inspection. The payload of the incoming MGCP signaling packet is inspected according to RFC 3435. Malformed packets are blocked.
- Stateful processing of MGCP sessions. State machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- MGCP Network Address Translation (NAT). Embedded IP addresses and ports in packet bodies is properly translated based on current routing information and network topology, and is replaced with the translated IP address and port number, if necessary.
- Manages pinholes for VoIP traffic. To keep the VoIP network secure, the IP address and port information used for media or signalling is identified by the session helper, and pinholes are dynamically created and closed during call setup.

ONC-RPC portmapper session helper (pmap)

Open Network Computing Remote Procedure Call (ONC-RPC) is a widely deployed remote procedure call system. Also called Sun RPC, ONC-RPC allows a program running on one host to call a program running on another. The transport address of an ONC-RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

To accept ONC-RPC sessions you must add a security policy with service set to any or to the ONC-RPC pre-defined service (which listens on TCP and UDP port number 111). The RPC portmapper session helper (called pmap) handles the dynamic transport address negotiation mechanisms of ONC-RPC.

PPTP session helper for PPTP traffic (pptp)

The PPTP session help supports port address translation (PAT) for PPTP traffic. PPTP provides IP security at the Network Layer. PPTP consists of a control session and a data tunnel. The control session runs over TCP and helps in establishing and disconnecting the data tunnel. The data tunnel handles encapsulated Point-to-Point Protocol (PPP) packets carried over IP.

To accept PPTP sessions that pass through the FortiGate unit you must add a security policy with service set to any or to the PPTP pre-defined service (which listens on IP port 47 and TCP port 1723). The pptp session helper listens on TCP port 1723.

PPTP uses TCP port 1723 for control sessions and Generic Routing Encapsulation (GRE) (IP protocol 47) for tunneling the encapsulated PPP data. The GRE traffic carries no port number, making it difficult to distinguish between two clients with the same public IP address. PPTP uses the source IP address and the Call ID field in the GRE header to identify a tunnel. When multiple clients sharing the same IP address establish tunnels with the same PPTP server, they may get the same Call ID. The call ID value can be translated in both the control message and the data traffic, but only when the client is in a private network and the server is in a public network.

PPTP clients can either directly connect to the Internet or dial into a network access server to reach the Internet. A FortiGate unit that protects PPTP clients can translate the clients' private IP addresses to a pool of public IP addresses using NAT port translation (NAT-PT). Because the GRE traffic carries no port number for address translation, the pptp session helper treats the Call ID field as a port number as a way of distinguishing multiple clients.

After the PPTP establishing a TCP connection with the PPTP server, the client sends a start control connection request message to establish a control connection. The server replies with a start control connection reply message. The client then sends a request to establish a call and sends an outgoing call request message. FortiOS assigns a Call ID (bytes 12-13 of the control message) that is unique to each PPTP tunnel. The server replies with an outgoing call reply message that carries its own Call ID in bytes 12-13 and the client's call ID in bytes 14-15. The pptp session helper parses the control connection messages for the Call ID to identify the call to which a specific PPP packet belongs. The session helper also identifies an outgoing call request message using the control message type field (bytes 8-9) with the value 7. When the session helper receives this message, it parses the control message for the call ID field (bytes 12-13). FortiOS translates the call ID so that it is unique across multiple calls from the same translated client IP. After receiving outgoing call response message, the session helper holds this message and opens a port that accepts GRE traffic that the PPTP server sends. An outgoing call request message contains the following parts:

- The protocol used for the outgoing call request message (usually GRE)
- Source IP address (PPTP server IP)
- Destination IP address (translated client IP)
- Destination port number (translated client call ID)

The session helper identifies an outgoing call reply message using the control message type field (bytes 8-9) with the value 8. The session helper parses these control messages for the call ID field (bytes 12-13) and the client's call ID (bytes 14-15). The session helper then uses the client's call ID value to find the mapping created for the other direction, and then opens a pinhole to accept the GRE traffic that the client sends.

An outgoing call reply message contains the following parts:

- Protocol used for the outgoing call reply message (usually GRE)
- Source IP address (PPTP client IP)
- Destination IP address (PPTP server IP)
- Destination port number (PPTP server Call ID)

Each port that the session opens creates a session for data traffic arriving in that direction. The session helper opens the following two data sessions for each tunnel:

- Traffic from the PPTP client to the server, using the server's call ID as the destination port
- Traffic from the PPTP server to the client, using the client's translated call ID as the destination port

The default timeout value of the control connection is 30 minutes. The session helper closes the pinhole when the data session exceeds the timeout value or is idle for an extended period.

Remote shell session helper (rsh)

Using the remote shell program (RSH), authenticated users can run shell commands on remote hosts. RSH sessions most often use TCP port 514. To accept RSH sessions you must add a security policy with service set to any or to the RSH pre-defined service (which listens on TCP port number 514).

FortiOS automatically invokes the rsh session helper to process all RSH sessions on TCP port 514. The rsh session helper opens ports required for the RSH service to operate through a FortiGate unit running NAT or transparent and supports port translation of RSH traffic.

Real-Time Streaming Protocol (RTSP) session helper (rtsp)

The Real-Time Streaming Protocol (RTSP) is an application layer protocol often used by SIP to control the delivery of multiple synchronized multimedia streams, for example, related audio and video streams. Although RTSP is capable of delivering the data streams itself it is usually used like a network remote control for multimedia servers. The protocol is intended for selecting delivery channels (like UDP, multicast UDP, and TCP) and for selecting a delivery mechanism based on the Real-Time Protocol (RTP). RTSP may also use the SIP Session Description Protocol (SDP) as a means of providing information to clients for aggregate control of a presentation consisting of streams from one or more servers, and non-aggregate control of a presentation consisting of multiple streams from a single server.

To accept RTSP sessions you must add a security policy with service set to any or to the RTSP pre-defined service (which listens on TCP ports 554, 770, and 8554 and on UDP port 554). The rtsp session helper listens on TCP ports 554, 770, and 8554.

The rtsp session help is required because RTSP uses dynamically assigned port numbers that are communicated in the packet body when end points establish a control connection. The session helper keeps track of the port numbers and opens pinholes as required. In Network Address Translation (NAT) mode, the session helper translates IP addresses and port numbers as necessary.

In a typical RTSP session the client starts the session (for example, when the user selects the Play button on a media player application) and establishes a TCP connection to the RTSP server on port 554. The client then sends an OPTIONS message to find out what audio and video features the server supports. The server responds to the OPTIONS message by specifying the name and version of the server, and a session identifier, for example, 24256-1.

The client then sends the DESCRIBE message with the URL of the actual media file the client wants to play. The server responds to the DESCRIBE message with a description of the media in the form of SDP code. The client

then sends the SETUP message, which specifies the transport mechanisms acceptable to the client for streamed media, for example RTP/RTCP or RDT, and the ports on which it receives the media.

In a NAT configuration the rtsp session helper keeps track of these ports and addresses translates them as necessary. The server responds to the SETUP message and selects one of the transport protocols. When both client and server agree on a mechanism for media transport the client sends the PLAY message, and the server begins streaming the media.

Session Initiation Protocol (SIP) session helper (sip)

The sip session helper is described in the VoIP Solutions: SIP Guide.

Trivial File Transfer Protocol (TFTP) session helper (tftp)

To accept TFTP sessions you must add a security policy with service set to any or to the TFTP pre-defined service (which listens on UDP port number 69). The TFTP session helper also listens on UTP port number 69.

TFTP initiates transfers on UDP port 69, but the actual data transfer ports are selected by the server and client during initialization of the connection. The tftp session helper reads the transfer ports selected by the TFTP client and server during negotiation and opens these ports on the firewall so that the TFTP data transfer can be completed. When the transfer is complete the tftp session helper closes the open ports.

Oracle TNS listener session helper (tns)

The Oracle Transparent Network Substrate (TNS) listener listens on port TCP port 1521 for network requests to be passed to a database instance. The Oracle TNS listener session helper (tns) listens for TNS sessions on TCP port 1521. TNS is a foundation technology built into the Oracle Net foundation layer and used by SQLNET.

Advanced concepts

This chapter provides configuration concepts and techniques to enhance your network security.

This section includes the topics:

- Dual internet connections (redundant Internet connections)
- Single firewall vs. multiple virtual domains
- Modem
- FortiExtender
- DHCP servers and relays
- Assigning IP address by MAC address
- DNS services
- Dynamic DNS
- FortiClient discovery and registration
- IP addresses for self-originated traffic
- Administration for schools
- Replacement messages list
- Disk
- CLI Scripts
- Rejecting PING requests
- Opening TCP 113
- Obfuscate HTTP responses

Dual internet connections (redundant Internet connections)

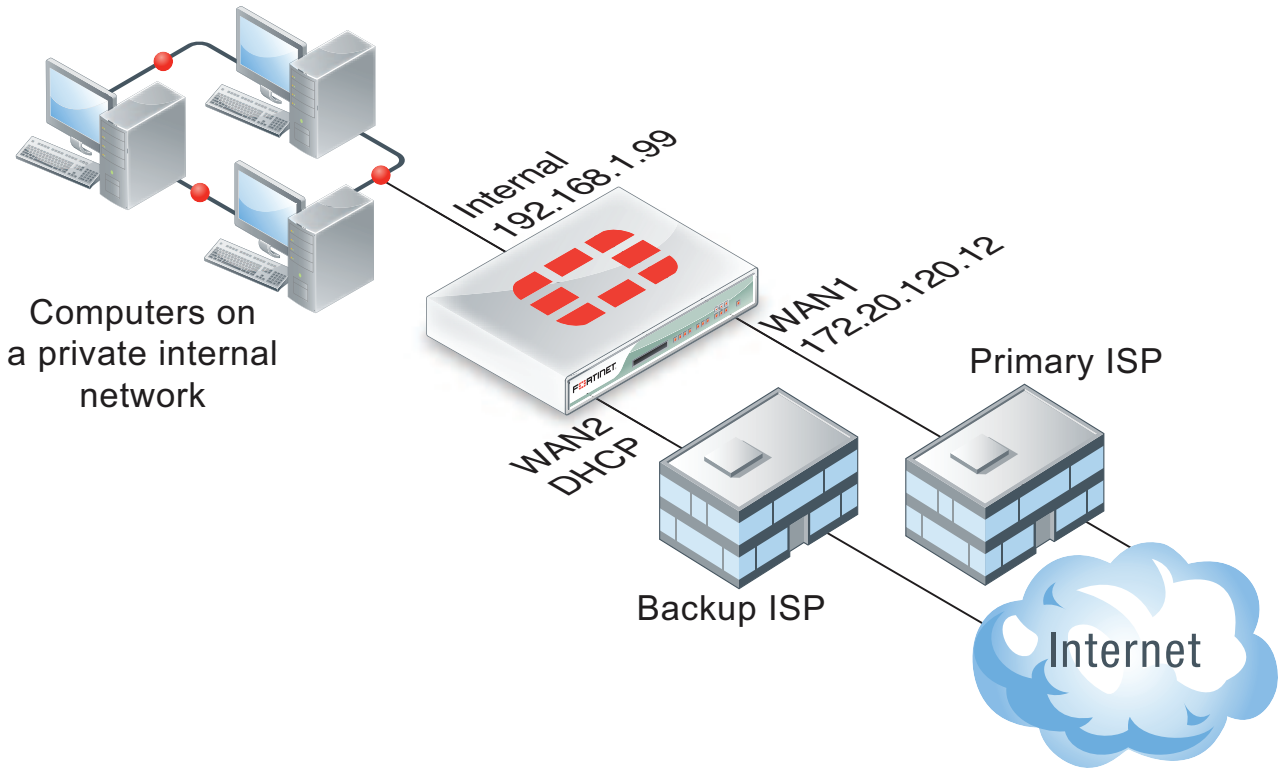
Dual internet connection, dual WAN, or redundant internet connection refers to using two FortiGate interfaces to connect to the Internet. Dual internet connections can be used in three ways:

- Redundant interfaces, should one interface go down, the second automatically becomes the main internet connection
- For load sharing to ensure better throughput.
- A combination of redundancy and load sharing.

Redundant interfaces

Redundant interfaces, ensures that should your internet access be no longer available through a certain port, the FortiGate unit will use an alternate port to connect to the Internet.

Configuring redundant interfaces



In this scenario, two interfaces, WAN1 and WAN2 are connected to the Internet using two different ISPs. WAN1 is the primary connection. In an event of a failure of WAN1, WAN2 automatically becomes the connection to the Internet. For this configuration to function correctly, you need to configure three specific settings:

- Configure a link health monitor to determine when the primary interface (WAN1) is down and when the connection returns
- Configure a default route for each interface.
- Configure security policies to allow traffic through each interface to the internal network.

Link Health Monitor

Adding a link health monitor is required for routing fail over traffic. A link health monitor will confirm the connectivity of the device's interface

To add a link health monitor - web-based manager

1. Go to **Router > Static > Settings** and select **Create New**.
   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Choose a name.
3. Select the **Interface** that will send probe requests.
4. Specify the **Gateway** IP address if required, if not keep it set to *0.0.0.0*.
5. Make sure that **Health Check** is enabled.
6. Set the **Probe Type** to **Ping** or **HTTP**.

7. For the **Server** field, enter the IP address of a server that the FortiGate unit will send ping or http requests to.
8. For the **Ping Interval**, enter the number of seconds to send ping requests.
9. For the **Failover Threshold**, enter the number of lost pings or http requests is acceptable before the port is determined to be down.
10. Make sure to enable **Update Routing Table when Gateway Detection Status Changes**.
11. Enable **Bring Down (Up)** and select **WAN2** interface.
12. Select **OK**.

To add a link health monitor - CLI

```
config system link-monitor
   edit "Example1"
      set srcint <Interface_sending_probe>
      set server <ISP_IP_address>
      set protocol <Ping or http>
      set gateway-ip <the_gateway_IP_to_reach_the_server_if_required>
      set failtime <failure_count>
      set interval <seconds>
      set update-cascade-interface enable
      set update-static-route enable
      set status enable
end
```

Routing

You need to configure a default route for each interface and indicate which route is preferred by specifying the distance. The lower distance is declared active and placed higher in the routing table.

When you have dual WAN interfaces that are configured to provide fail over, you might not be able to connect to the backup WAN interface because the FortiGate unit may not route traffic (even responses) out of the backup interface. The FortiGate unit performs a reverse path lookup to prevent spoofed traffic. If no entry can be found in the routing table which sends the return traffic out the same interface, then the incoming traffic is dropped.

To configure the routing of the two interfaces - web-based manager

1. Go to **Router > Static > Static Routes** and select **Create New Route** or **IPv6 Route**.
   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New Route** or **IPv6 Route**.
2. Set the **Destination IP/Mask** to the address and netmask of 0.0.0.0/0.0.0.0 if it's an IPv4 route. If it's an IPv6 route, set **Destination IP/Mask** to the address and netmask of ::/0
3. Select the **Device** to the primary connection, **WAN1**.
4. Enter the **Gateway** address.
5. Select **Advanced**.
6. Set the **Distance** to `10`.
7. Select **OK**.
8. Repeat steps 1 through 7 setting the **Device** to **WAN2** and a **Distance** of `20`.

To configure the IPv4 routing of the two interfaces - CLI

```
config router static
   edit 0
      set dst 0.0.0.0 0.0.0.0
      set device WAN1
      set gateway <gateway_address>
      set distance 10
   next
   edit 0
      set dst 0.0.0.0 0.0.0.0
      set device WAN2
      set gateway <gateway_address>
      set distance 20
   next
end
```

To configure the IPv6 routing of the two interfaces - CLI

```
config router static6
   edit 0
      set dst ::/0
      set device WAN1
      set gateway <gateway_address>
      set distance 10
   next
   edit 0
      set dst ::/0
      set device WAN2
      set gateway <gateway_address>
      set distance 20
   next
end
```

Security policies

When creating security policies, you need to configure duplicate policies to ensure that after traffic fails over WAN1, regular traffic will be allowed to pass through WAN2 as it did with WAN1. This ensures that fail-over will occur with minimal affect to users. For more information on creating security policies see the Firewall Guide.

Load sharing

Load sharing enables you to use both connections to the internet at the same time, but do not provide fail over support. When configuring for load sharing, you need to ensure routing is configured for both external ports, for example, WAN1 and WAN2, have static routes with the same distance and priority.

Further configuration can be done using Equal Cost Multiple Path (ECMP). For more information on ECMP and load sharing, see the Advanced Routing Guide.

Link redundancy and load sharing

In this scenario, both links are available to distribute Internet traffic over both links. Should one of the interfaces fail, the FortiGate unit will continue to send traffic over the other active interface. Configuration is similar to the

Redundant interfaces configuration, with the main difference being that the configured routes should have equal distance settings.

This means both routes will remain active in the routing table. To make one interface the preferred interface, use a default policy route to indicate the interface that is preferred for accessing the Internet. If traffic matches the security policy, the policy overrides all entries in the routing table, including connected routes. You may need to add a specific policy routes that override these default policy routes.

To redirect traffic over the secondary interface, create policy routes to direct some traffic onto it rather than the primary interface. When adding the policy route, only define the outgoing interface and leave the gateway blank. This ensures that the policy route will not be active when the link is down.

Single firewall vs. multiple virtual domains

A typical FortiGate setup, with a small to mid-range appliance, enables you to include a number of subnets on your network using the available ports and switch interfaces. This can potentially provide a means of having three or more mini networks for the various groups in a company. Within this infrastructure, multiple network administrators have access to the FortiGate to maintain security policies.

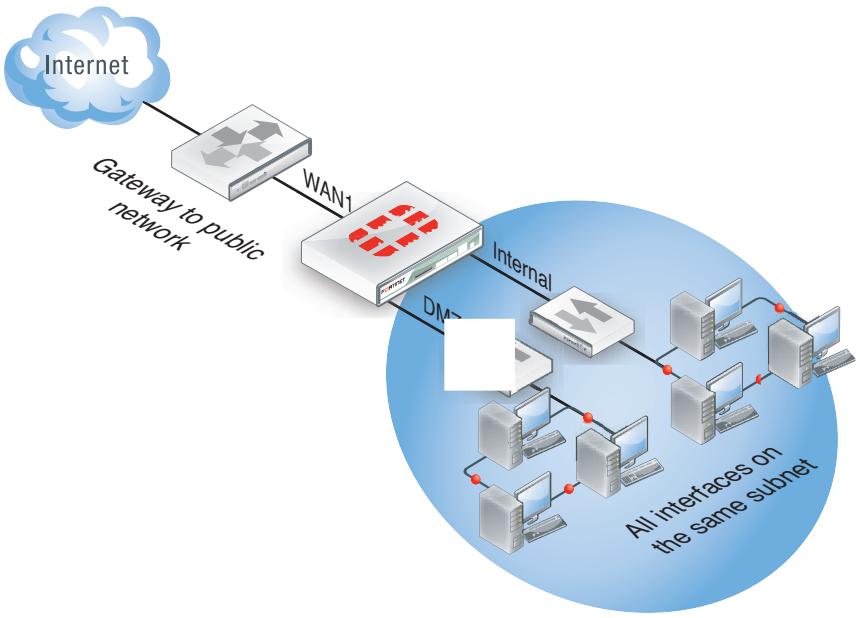
However, the FortiGate unit may not have enough interfaces to match the number of departments in the organization. If the FortiGate unit it running in transparent mode however, there is only one interface, and multiple network branches through the FortiGate are not possible.

A FortiGate unit with Virtual Domains (VDOMs) enabled, provides a means to provide the same functionality in transparent mode as a FortiGate in NAT mode. VDOMs are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network. For administration, an administrator can be assigned to each VDOM, minimizing the possibility of error or fouling network communications.

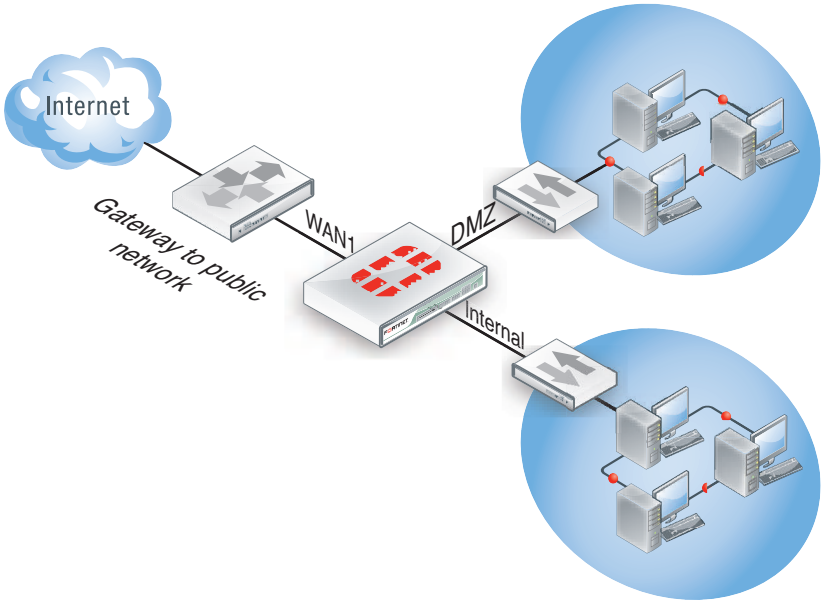
By default, most FortiGate units support 10 VDOMs. Many FortiGate models support purchasing a license key to increase the maximum number.

Single firewall vs. vdoms

When VDOMs are not enabled, and the FortiGate unit is in transparent mode, all the interfaces on your unit become broadcast interfaces. The problem is there are no interfaces free for additional network segments.



A FortiGate with three interfaces means only limited network segments are possible without purchasing more FortiGate devices.



With multiple VDOMs you can have one of them configured in transparent mode, and the rest in NAT mode. In this configuration, you have an available transparent mode FortiGate unit you can drop into your network for troubleshooting, and you also have the standard.

This example shows how to enable VDOMs on the FortiGate unit and the basic and create a VDOM accounting on the DMZ2 port and assign an administrator to maintain the VDOM. First enable Virtual Domains on the FortiGate unit.

To enable VDOMs - web-based manager

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select **Enable** for **Virtual Domain**.

Note that on FortiGate-60 series and lower models, you need to enable VDOMs in the CLI only.

The FortiGate unit logs you out. Once you log back in, you will notice that the menu structure has changed. This reflects the global settings for all Virtual Domains.

To enable VDOMs - CLI

```
config system global
   set vdom-admin enable
end
```

Next, add the VDOM called accounting.

To add a VDOM - web-based manager

1. Go to **Global > VDOM > VDOM**, and select **Create New**.
2. Enter the VDOM name `accounting`.
3. Select **OK**.

To add a VDOM - CLI

```
config vdom
   edit <new_vdom_name>
end
```

With the Virtual Domain created, you can assign a physical interface to it, and assign it an IP address.

To assign physical interface to the accounting Virtual Domain - web-based manager

1. Go to **Global > Network > Interface**.
2. Select the DMZ2 port row and select **Edit**.
3. For the **Virtual Domain** drop-down list, select **accounting**.
4. Select the **Addressing Mode** of **Manual**.
5. Enter the IP address for the port of 10.13.101.100/24.
6. Set the **Administrative Access** to **HTTPS** and **SSH**.
7. Select **OK**.

To assign physical interface to the accounting Virtual Domain - CLI

```
config global
   config system interface
      edit dmz2
      set vdom accounting
      set ip 10.13.101.100/24
      set allowaccess https ssh
   next
end
```

Modem

FortiGate units support the use of wireless, 3G and 4G modems connected using the USB port or, if available, the express card slot. Modem access provides either primary or secondary (redundant) access to the Internet. For FortiGate units that do not include an internal modem (those units with an “M” designation), the modem interface will not appear in the web-based manager until enabled in the CLI. To enable the modem interface enter the CLI commands:

```
config system modem
   set status enable
end
```

You will need to log out of the FortiGate and log back in to see the modem configuration page at **System > Network > Modem**. Once enabled, modem options become available by going to **System > Network > Interface**.

Note that the modem interface is only available when the FortiGate unit is in NAT mode.

To configure modem settings, go to **System > Network > Modem**.

Configuring the modem settings is a matter of entering the ISP phone number, user name and password. Depending on the modem, additional information may need to be supplied such as product identifiers, and initialization strings.

The FortiGate unit includes a number of common modems within its internal database. You can view these by selecting the **Configure Modem** link on the **Modem Settings** page. If your modem is not on the list, select **Create New** to add the information. This information is stored on the device, and will remain after a reboot.

Fortinet has an online database of modem models and configuration settings through FortiGuard. A subscription to the FortiGuard services is not required to access the information. As models are added, you can select the **Configure Modem** link and select **Update Now** to download new configurations.

USB modem port

Each USB modem has a specific dial-out port. This will be indicated with the documentation for your modem. To enable the correct USB port, use the CLI commands:

```
config system modem
   set wireless-port {0 | 1 | 2}
end
```

To test the port, use the diagnose command:

```
diagnose sys modem com /1
```

The 1 will be the value of your USB port selected. The response will be:

```
Serial port: /dev/1
Press Ctrl+W to exit.
```

If the port does not respond the output will be:

```
Can not open modem device '/dev/1' : Broken pipe
```

Modes

The FortiGate unit allows for two modes of operation for the modem; stand alone and redundant. In stand alone mode, the modem connects to a dialup ISP account to provide the connection to the Internet. In redundant mode, the modem acts as a backup method of connecting to the Internet, should the primary port for this function fails.

Configuring either stand alone or redundant modes are very similar. The primary difference is the selection of the interface that the modem will replace in the event of it failing, and the configuration of a PING server to monitor the chosen interface.

Configuring stand alone mode

Configuring stand alone mode is a matter of configuring the modem information and the dialing mode. The dial mode is either **Always Connect** or **Dial on demand**. Selecting **Always Connect** ensures that once the modem has connected, it remains connected to the ISP. Selecting **Dial on Demand**, the modem only calls the ISP if packets are routed to the modem interface. Once sent, the modem will disconnect after a specified amount of time.

To configure standalone mode as needed - web-based manager

1. Go to **System > Network > Modem**.
2. Select the **Mode** of **Standalone**.
3. Select the **Dial Mode** of **Dial on Demand**.
4. Select the number of redials the modem attempts if connection fails to 5.
5. Select **Apply**.

To configure standalone mode as needed- CLI

```
config system modem
   set status enable
   set mode standalone
   set auto-dial enable
   set redial 5
end
```

Configuring redundant mode

Redundant mode provides a backup to an interface, typically to the Internet. If that interface fails or disconnects, the modem automatically dials the configured phone number(s). Once connected, the FortiGate unit routes all traffic to the modem interface until the monitored interface is up again. The FortiGate unit pings the connection to determine when it is back online.

For the FortiGate to verify when the interface is back up, you need to configure a Ping server for that interface. You will also need to configure security policies between the modem interface and the other interfaces of the FortiGate unit to ensure traffic flow.

To configure redundant mode as needed - web-based manager

1. Go to **System > Network > Modem**.
2. Select the **Mode** of **Redundant**.

3. Select the interface the modem takes over from if it fails.
4. Select the **Dial Mode** of **Dial on Demand**.
5. Select the number of redials the modem attempts if connection fails to 5.
6. Select **Apply**.

To configure standalone mode as needed- CLI

```
config system modem
   set status enable
   set mode redundant
   set interface wan1
   set auto-dial enable
   set redial 5
end
```

Link Health Monitor

Adding a link health monitor is required for routing fail over traffic. A link health monitor will confirm the connectivity of the device's interface

To add a link health monitor - web-based manager

1. Go to **Router > Static > Settings** and select **Create New**.
   For low-end FortiGate units, go to **System > Network > Routing** and select **Create New**.
2. Choose a name.
3. Select the **Interface** that will send probe requests which is the modem.
4. Specify the **Gateway** IP address if required, if not keep it set to *0.0.0.0*.
5. Make sure that **Health Check** is enabled.
6. Set the **Probe Type** to **Ping** or **HTTP**.
7. For the **Server** field, enter the IP address of a server that the FortiGate unit will send ping or http requests to.
8. For the **Ping Interval**, enter the number of seconds to send ping requests.
9. For the **Failover Threshold**, enter the number of lost pings or http requests is acceptable before the port is determined to be down.
10. Make sure to enable **Update Routing Table when Gateway Detection Status Changes**.
11. Enable **Bring Down (Up)** and select the redundant interface.
12. Select **OK**.

To add a link health monitor - CLI

```
config system link-monitor
   edit "Example1"
      set srcint <Interface_sending_probe>
      set server <ISP_IP_address>
      set protocol <Ping or http>
      set gateway-ip <the_gateway_IP_to_reach_the_server_if_required>
      set failtime <failure_count>
      set interval <seconds>
      set update-cascade-interface enable
      set update-static-route enable
      set status enable
end
```

Additional modem configuration

The CLI provides additional configuration options when setting up the modem options including adding multiple ISP dialing and initialization options and routing. For more information, see the CLI Reference.

Modem interface routing

The modem interface can be used in FortiOS as a dedicated interface. Once enabled and configured, you can use it in security policies and define static and dynamic routing. Within the CLI commands for the modem, you can configure the distance and priority of routes involving the modem interface. The CLI commands are:

```
config sysetm modem
   set distance <route_distance>
   set priority <priority_value>
end
```

For more information on the routing configuration in the CLI, see the CLI Reference. For more information on routing and configuring routing, see the Advanced Routing Guide.

FortiExtender

FortiGate units support the use of wireless, 3G and 4G modems connected to a FortiExtender which will be connected to the FortiGate unit.

Installing the 3G/4G modem

Remove the housing cover of the FortiExtender and use the provided USB extension cable to connect your 3G/4G modem to the device.

For more information on installing the 3G/4G modem, see the QuickStart Guide.

Connecting the FortiExtender unit

If you are using the provided PoE injector:

1. Plug the provided Ethernet cable into the Ethernet port of the FortiExtender and insert the other end of the Ethernet cable into the AP/Bridge port on the injector, then plug the injector into an electrical outlet.
2. Connect the LAN port of the PoE injector to a FortiGate, FortiWifi, or FortiSwitch device.

If you are not using the PoE injector:

1. Insert the other end of the Ethernet cable into a PoE LAN port on an appropriate FortiGate, FortiWifi or FortiSwitch device.

For more information on connecting the FortiExtender unit, see the QuickStart Guide.

Once connected, your FortiGate appliance can automatically detect, connect with, and control the FortiExtender and modem via a CAPWAP tunnel.To do this, FortiExtender and FortiGate must be on the same Layer 2/3 subnet (or have DHCP relay between) and FortiGate must respond to FortiExtender's request. In this example FortiExtender is connected to the ***lan*** interface of the FortiGate unit.

By default, FortiExtender is hidden and disabled.Enable it in FortiGate's CLI:

```
config system global
   set fortiextender enable
```

```
    set wireless-cotnroller enable
end
```

The control and provisioning of Wireless Access Point (CAPWAP) service must be enabled on the port to which the FortiExtender unit is connected (***lan*** interface in this example) using the following CLI commands:

```
config system interface
   edit lan
   append allowaccess capwap
end
```

Once FortiExtender is discovered and authorized, a virtual WAN interface such as ***fext-wan1*** is created on the Fortigate.

Configuring the FortiExtender unit

At this point, you can fully manage the FortiExtender from the FortiGate unit. To achieve this, you need to authorize the FortiExtender by going to ***System > Network > FortiExtender*** and click on ***Authorize.*** Once authorized, you can configure you device as required:

Link Status: Shows you if the link is ***Up*** or ***Down,*** click on ***Details*** to see the System and Modem Status.

IP Address: Shows you the current FortiExtender's IP address, click on the link of the IP address to connect to the FortiExtender GUI.

OS Version: Shows the current FortiExtender's build, click on ***Upgrade*** if you wish to upgrade the Firmware.

Configure Settings: Allows you to configure the Modem Settings, PPP Authentication, General, GSM / LTE, and CDMA.

Diagnostics: Allows you to diagnose the FortiExtender unit, you can choose a command form the existing commands and click on ***Run***.

Existing commands are: `Show device info, Show data session connection status, test connection, test disconnection, Get signal strength, AT Command.`

Simple output of `Show device info:`

```
Manufacturer: Sierra Wireless, Incorporated
Model: AirCard 330U
Revision: SWI9200X_03.00.08.03AP R4019 CARMD-EN-10527 2011/12/07 18:43:13
IMEI: 359615040996060
IMEI SV: 7
FSN: CDU3153118210
3GPP Release 8
+GCAP: +CGSM
OK
```

Modem Settings

The FortiExtender unit allows for two modes of operation for the modem; ***On Demand*** and ***Always Connect***.

In ***On Demand*** mode, the modem connects to an ISP only upon execution of the dial up operation and disconnects only upon subsequent hang up operation from the CLI.

Syntax

To connect, run the following CLI command:

```
execute extender dial <SN>  // <SN> is the FortiExtender's serial number.
```

To disconnect, run the following CLI command:

```
execute extender hangup <SN> // <SN> is the FortiExtender's serial number.
```

In ***Always Connect*** mode, the modem is always connected to the internet, it can acts as a primary or backup method of connecting to the Internet.

By default, the Fortiextender will be in ***Always Connect*** mode once authorized.

Modem Settings is a matter of configuring the dialing mode. The ***dial mode*** is either ***Always Connect*** or ***On demand***. Selecting ***Always Connect*** ensures that once the modem has connected, it remains connected to the ISP.

To configure the dial mode as needed - web-based manager

1. Go to ***System > Network > FortiExtender*** and click ***Configuring Settings***.
2. Extend ***Modem Settings***.
3. Select the ***Dial Mode*** of ***Always Connect*** or ***On Demand***.
4. Enter the ***Redial Limit*** to 5 - Only applicable in ***On Demand*** mode.
5. If needed, enter the ***Quota Limit*** to the desired limit in Mega Byte -The recorded quota usage values are not persistent and lost upon rebooting Fortigate.
6. Select ***Ok***.

Configuring the FortiGate unit

In order to allow inbound and outbound traffic through the 3G/4G modem, you need to add a security policy and, depending the scenario, a static route in the FortiGate unit.

Adding a policy

If your network will be using IPv4 addresses, go to ***Policy & Objects > Policy > IPv4*** and select ***Create New*** to add a policy that allows users on the private network to access the Internet.

In the policy, set the ***Incoming Interface*** to the internal interface and the ***Outgoing Interface*** to ***fext-wan1*** interface. You will also need to set ***Source Address***, ***Destination Address***, ***Schedule***, and ***Service*** according to your network requirements.

Make sure the ***Action*** is set to ***ACCEPT***. Turn on ***NAT*** and make sure ***Use Destination Interface Address*** is selected. Select ***OK.***

Always-on, redundant of wan1

No route required as in FortiOS 5.2.2 the routing shows only active routes.

Use the following CLI command to show all routes:

```
get router info routing-table all
```

Sample Output

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] via 172.20.120.2, wan1
C 25.49.248.0/24 is directly connected, fext-wan1
C 169.254.1.1/32 is directly connected, ssl.root
is directly connected, ssl.root
C 172.20.120.0/24 is directly connected, wan1
C 192.168.1.0/24 is directly connected, lan
```

Always-on, with select traffic going through the FortiExtender

In this scenario, a static route is required, if your network using IPv4 addresses, go to ***Router > Static > Static Routes*** or ***System > Network > Routing***, depending on your FortiGate model, and select ***Create New***. Set the ***Destination IP/Mask*** to 0.0.0.0/0.0.0.0, ***Device*** to ***fext-wan1***, and set the ***Gateway*** to your gateway IP or to the next hop router, depending on your network requirements. Select ***OK.***

ECMP across fext-wan1 and wan1

Go to ***Router > Static > Settings*** to configure ***ECMP Load Balancing Method***, choose between ***Source IP based, Weighted Load Balance, Spillover, Source-Destination IP based*** and configure your settings as required.

Go to ***System > Network > Interfaces*** and edit ***fext-wan1***, set the ***distance*** to the same distance as wan1 interface under ***Router > Static > Static Routes*** (in this example distance =10)

Now the traffic is shared between ***wan1*** and ***fext-wan1*** links respecting the ***ECMP Load Balancing Method*** used.

This deployment can be extrapolated for dual FortiExtender installation.

DHCP servers and relays

Note that DHCP server options are not available in transparent mode.

A DHCP server provides an address to a client on the network, when requested, from a defined address range.

An interface cannot provide both a server and a relay for connections of the same type (regular or IPsec). However, you can configure a Regular DHCP server on an interface only if the interface is a physical interface with a static IP address. You can configure an IPsec DHCP server on an interface that has either a static or a dynamic IP address.

You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

If an interface is connected to multiple networks via routers, you can add a DHCP server for each network. The IP range of each DHCP server must match the network address range. The routers must be configured for DHCP relay.

You can configure a FortiGate interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the unit.

DHCP Server configuration

To add a DHCP server, go to **System > Network > Interface**. Edit the interface, and select **Enable** for the **DHCP Server** row.

DHCP Server IP	This appears only when **Mode** is **Relay**. Enter the IP address of the DHCP server where the FortiGate unit obtains the requested IP address.
Address Range	By default, the FortiGate unit assigns an address range based on the address of the interface for the complete scope of the address. For example, if the interface address is 172.20.120.230, the default range created is 172.20.120.231 to 172.20.120.254. Select the range and select **Edit** to adjust the range as needed, or select **Create New** to add a different range.
Netmask	Enter the netmask of the addresses that the DHCP server assigns.
Default Gateway	Select to either use the same IP as the interface or select **Specify** and enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS Server	Select to use the system's DNS settings or select **Specify** and enter the IP address of the DNS server.
Advanced... (expand to reveal more options)	
Mode	Select the type of DHCP server the FortiGate unit will be. By default, it is a server. Select **Relay** if needed. When **Relay** is selected, the above configuration is replaced by a field to enter the **DHCP Server IP** address.
Type	Select to use the DHCP in regular or IPsec mode.
MAC Address Access Control List	Select to match an IP address from the DHCP server to a specific client or device using its MAC address. In a typical situation, an IP address is assigned ad hoc to a client, and that assignment times out after a specific time of inactivity from the client, known as the lease time. To ensure a client or device always has the same IP address, that is, there is no lease time, use IP reservation.
Add from DHCP Client List	If the client is currently connected and using an IP address from the DHCP server, you can select this option to select the client from the list.

DHCP in IPv6

You can use DHCP with IPv6 using the CLI. To configure DHCP, ensure IPv6 is enabled by going to **System > Config > Features** and enable **IPv6**. Use the CLI command

```
config system dhcp6 server
```

For more information on the configuration options, see the CLI Reference.

Service

On low-end FortiGate units, a DHCP server is configured, by default on the Internal interface:

IP Range	192.168.1.110 to 192.168.1.210
Netmask	255.255.255.0
Default gateway	192.168.1.99
Lease time	7 days
DNS Server 1	192.168.1.99

These settings are appropriate for the default Internal interface IP address of 192.168.1.99. If you change this address to a different network, you need to change the DHCP server settings to match.

Alternatively, after the FortiGate unit assigns an address, you can go to **System > Monitor > DHCP Monitor**, locate the particular user. Select the check box for the user and select **Add to Reserved**.

Lease time

The lease time determines the length of time an IP address remains assigned to a client. Once the lease expires, the address is released for allocation to the next client request for an IP address The default lease time is seven days. To change the lease time, use the following CLI commands:

```
config system dhcp server
   edit <server_entry_number>
      set lease-time <seconds>
   end
```

To have an unlimited lease time, set the value to zero.

DHCP options

When adding a DHCP server, you have the ability to include DHCP codes and options. The DHCP options are BOOTP vendor information fields that provide additional vendor-independent configuration parameters to manage the DHCP server. For example, you may need to configure a FortiGate DHCP server that gives out a separate option as well as an IP address. For example, an environment that needs to support PXE boot with Windows images.

The option numbers and codes are specific to the particular application. The documentation for the application will indicate the values to use. Option codes are represented in a option value/HEX value pairs. The option is a value 1 and 255.

You can add up to three DHCP code/option pairs per DHCP server.

To configure option 252 with value http://192.168.1.1/wpad.dat - CLI

```
config system dhcp server
   edit <server_entry_number>
      set option1 252 687474703a2f2f3139322e3136382e312e312f777061642e646174
end
```

For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions.

Exclude addresses in DHCP a range

If you have a large address range for the DHCP server, you can block a range of addresses that will not be included in the available addresses for the connecting users. To do this, go to the CLI and enter the commands:

```
config system dhcp server
   edit <server_entry_number>
      config exclude-range
         edit <sequence_number>
            set start-ip <address>
            set end-ip <address>
         end
      end
   end
```

DHCP Monitor

To view information about DHCP server connections, go to **System > Monitor > DHCP Monitor**. On this page, you can also add IP address to the reserved IP address list.

Breaking an address lease

Should you need to end an IP address lease, you can break the lease using the CLI. This is useful if you have limited addresses, longer lease times where leases are no longer necessary. For example, with corporate visitors.

To break a lease enter the CLI command:

```
execute dhcp lease-clear <ip_address>
```

Assigning IP address by MAC address

To prevent users in the from changing their IP addresses and causing IP address conflicts or unauthorized use of IP addresses, you can bind an IP address to a specific MAC address using DHCP.

Use the CLI to reserve an IP address for a particular client identified by its device MAC address and type of connection. The DHCP server then always assigns the reserved IP address to the client. The number of reserved addresses that you can define ranges from 10 to 200 depending on the FortiGate model.

After setting up a DHCP server on an interface by going to **System > Network > Interface**, select the blue arrow next to **Advanced** to expand the options. If you know the MAC address of the system select **Create New** to add it, or if the system has already connected, locate it in the list, select its check box and select A**dd from DHCP Client List**.

You can also match an address to a MAC address in the CLI. In the example below, the IP address 10.10.10.55 is assigned to MAC address 00:09:0F:30:CA:4F.

```
config system dhcp server
   edit 1
      config reserved-address
         edit 1
            set ip 10.10.10.55
            set mac 00:09:0F:30:CA:4F
end
```

DNS services

A DNS server is a public service that converts symbolic node names to IP addresses. A Domain Name System (DNS) server implements the protocol. In simple terms, it acts as a phone book for the Internet. A DNS server matches domain names with the computer IP address. This enables you to use readable locations, such as fortinet.com when browsing the Internet. FortiOS supports DNS configuration for both IPv4 and IPv6 addressing.

The FortiGate unit includes default DNS server addresses. However, these should be changed to those provided by your Internet Service Provider. The defaults are DNS proxies and are not as reliable as those from your ISP.

Within FortiOS, there are two DNS configuration options; each provide a specific service, and can work together to provide a complete DNS solution.

DNS settings

Basic DNS queries are configured on interfaces that connect to the Internet. When a website is requested, for example, the FortiGate unit will look to the configured DNS servers to provide the IP address to know which server to contact to complete the transaction.

DNS server addresses are configured by going to **System > Network > DNS**. Here you specify the DNS server addresses. Typically, these addresses are supplied by your ISP. An additional option is available if you have local Microsoft domains on the network, by entering a domain name in the **Local Domain Name** field.

In a situation where all three fields are configured, the FortiGate unit will first look to the local domain. If no match is found, a request is sent to the external DNS servers.

If virtual domains are enabled, you create a DNS database in each VDOM. All of the interfaces in a VDOM share the DNS database in that VDOM.

Additional DNS CLI configuration

Further options are available from the CLI with the command `config system dns`. Within this command you can set the following commands:

- `dns-cache-limit` - enables you to set how many DNS entries are stored in the cache. Entries that remain in the cache provide a quicker response to requests than going out to the Internet to get the same information.
- `dns-cache-ttl` - enables you to set how long entries remain in the cache in seconds, between 60 and 86,400 (24 hours).
- `cache-notfound-responses` - when enabled, any DNS requests that are returned with NOTFOUND can be stored in the cache.
- `source-ip` - enables you to define a dedicated IP address for communications with the DNS server.

DNS server

You can also create local DNS servers for your network. Depending on your requirements, you can manually maintain your entries (master DNS server), or use it as a jumping point, where the server refers to an outside source (slave DNS server). A local master DNS server works similarly to the DNS server addresses configured in ***System > Network > DNS***, but all entries must be added manually. This enables you to add a local DNS server to include specific URL/IP address combinations.

The DNS server options are not visible in the web-based manager by default. To enable the server, go to ***System > Config > Features*** and select ***DNS Database***.

While a master DNS server is an easy method of including regularly used addresses to save on going to an outside DNS server, it is not recommended to make it the authoritative DNS server. IP addresses may change, and maintaining any type of list can quickly become labor-intensive.

A FortiGate master DNS server is best set for local services. For example, if your company has a web server on the DMZ that is accessed by internal employees as well as external users, such as customers or remote users. In this situation, the internal users when accessing the site would send a request for website.example.com, that would go out to the DNS server on the web, to return an IP address or virtual IP. With an internal DNS, the same site request is resolved internally to the internal web server IP address, minimizing inbound/outbound traffic and access time.

As a slave, DNS server, the FortiGate server refers to an external or alternate source as way to obtain the url/IP combination. This useful if there is a master DNS server for a large company where a list is maintained. Satellite offices can then connect to the master DNS server to obtain the correct addressing.

The DNS server entries does not allow CNAME entries, as per RFC 1912, section 2.4.

To configure a master DNS server - web-based manager

1. Go to ***System > Network > DNS Server***, and select ***Create New*** for ***DNS Database***.
2. Select the ***Type*** of ***Master***.
3. Select the ***View*** as ***Shadow***.
4. The view is the accessibility of the DNS server. Selecting ***Public***, external users can access, or use, the DNS server. Selecting ***Shadow***, only internal users can use it.
5. Enter the DNS ***Zone***, for example, `WebServer`.
6. Enter the domain name for the zone, for example `example.com`.
7. Enter the hostname of the DNS server, for example, `Corporate`.
8. Enter the contact address for the administrator, for example, `admin@example.com`.
9. Set ***Authoritative*** to ***Disable***.
10. Select ***OK***.
11. Enter the DNS entries for the server by selecting ***Create New***.
12. Select the ***Type***, for example, ***Address (A)***.
13. Enter the ***Hostname***, for example `web.example.com`.
14. Enter the remaining information, which varies depending on the **Type** selected.
15. Select ***OK***.

To configure a DNS server - CLI

```
config system dns-database
   edit WebServer
      set domain example.com
      set type master
      set view shadow
      set ttl 86400
      set primary-name corporate
      set contact admin@exmple.com
      set authoritative disable
         config dns-entry
            edit 1
               set hostname web.example.com
               set type A
               set ip 192.168.21.12
```

```
            set status enable
        end
    end
```

Recursive DNS

You can set an option to ensure these types of DNS server is not the authoritative server. When configured, the FortiGate unit will check its internal DNS server (Master or Slave). If the request cannot be fulfilled, it will look to the external DNS servers. This is known as a split DNS configuration.

You can also have the FortiGate unit look to an internal server should the Master or Slave not fulfill the request by using the CLI commands:

```
config system dns-database
   edit example.com
      ...
      set view shadow
end
```

For this behavior to work completely, for the external port, you must set the DNS query for the external interface to be recursive. This option is configured in the CLI only.

To set the DNS query

```
config system dns-server
   edit wan1
      set mode recursive
end
```

Dynamic DNS

If your ISP changes your external IP address on a regular basis, and you have a static domain name, you can configure the external interface to use a dynamic DNS service to ensure external users and/or customers can always connect to your company firewall.

If you have a FortiGuard subscription, you can use FortiGuard as your DDNS server. To configure dynamic DNS in the web-based manager, go to ***System > Network > DNS***, select ***Enable FortiGuard DDNS***, and enter the relevant information for the interface communicating to the server, and which server to use, and relevant information.

If you do not have a FortiGuard subscription, or want to use an alternate server, you can configure dynamic DNS in the CLI use the commands below. Within the CLI you can configure a DDNS for each interface. Only the first configured port appears in the web-based manager. Additional commands vary with the DDNS server you select.

```
config system ddns
   edit <instance_value>
      set monitor-interface <external_interface>
      set ddns-server <ddns_server_selection>
end
```

You can also use FortiGuard (when subscribed) as a DDNS as well. To configure, use the CLI commands:

```
config system fortiguard
   set ddns-server-ip
   set ddns-server-port
end
```

FortiClient discovery and registration

FortiOS provides a means of allowing users running FortiClient Endpoint Control software to connect to specific interfaces when connecting to the FortiGate unit. As well as ensuring that remote or local users have FortiClient Endpoint Control software installed on their PC or mobile device.

FortiClient discovery

You can configure a FortiGate interface as an interface that will accept FortiClient connections. When configured, the FortiGate unit sends broadcast messages which the FortiClient software running on an end user PC is listening for.

To enable the broadcast message

1. Go to ***System > Network > Interface***.
2. Edit the interface to send the broadcast messages.
3. Select **FCT-Access**.
4. In **Device Management**, select **Broadcast Discovery Messages**.
5. Select **OK**.

Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message.

You also have the option of including a registration key. When the FortiClient discovers the FortiGate unit, it is prompted to enter a registration key, defined by the administrator.

To add a registration key

1. Go to **System > Config > Advanced**.
2. Select **Enable Registration Key for FortiClient**, and enter the key.
3. Select **Apply**.

Ensure you distribute the key to the users that need to connect to the FortiGate unit.

FortiClient Registration

On the end user side, if FortiClient has not been registered with the FortiGate unit, it is continually listening for the FortiGate discovery message. When this message is detected the un-registered client will pop-up a FortiGate Detected message. The user can choose to either register or ignore the message.

Clients that have registered with that FortiGate unit will not be listening for these messages and will not display the message again.

If you enabled the registration key, the user is prompted to enter the key before a connection can be completed.

There can be some confusion when discussing the compatibility of FortiClient with FortiGate. There is technical compatibility and licensing compatibility. FortiClient software may not be licence compatible with previous versions of FortiOS.

For instance, while FortiClient 5.2 software is technologically compatible with a FortiGate running FortiOS 5.0 firmware. A FortiGate running FortiOS 5.0 will not recognize the FortiClient 5.2 licence code. Depending on the restrictions of your particular situation, you can:

- Use FortiClient 5.2 without licensing
- Use FortiClient 5.0 with licensing
- Upgrade to FortiOS firmware 5.2

For more information on FortiGate registration, see the FortiClient Administration Guide.

IP addresses for self-originated traffic

On the FortiGate unit, there are a number of protocols and traffic that is specific to the internal workings of FortiOS. For many of these traffic sources, you can identify a specific port/IP address for this self-originating traffic. The following traffic can be configured to a specific port/IP address:

- SNMP
- Syslog
- alert email
- FortiManager connection IP
- FortiGuard services
- FortiAnalyzer logging
- NTP
- DNS
- Authorization requests such as RADIUS
- FSSO

Configuration of these services is performed in the CLI. In each instance, there is a command set `source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
   set ntpsync enable
   set syncinterval 5
   set source-ip 192.168.4.5
end
```

To see which services are configured with source-ip settings, use the get command:

```
get system source-ip status
```

The output will appear similar to the sample below:

```
NTP: x.x.x.x
DNS: x.x.x.x
SNMP: x.x.x.x
Central Management: x.x.x.x
```

```
FortiGuard Updates (AV/IPS): x.x.x.x
FortiGuard Queries (WebFilter/SpamFilter): x.x.x.x
```

Administration for schools

For system administrator in the school system it is particularly difficult to maintain a network and access to the Internet. There are potential legal liabilities if content is not properly filtered and children are allowed to view pornography and other non-productive and potentially dangerous content. For a school, too much filtering is better than too little. This section describes some basic practices administrators can employ to help maintain control without being too draconian for access to the internet.

Security policies

The default security policies in FortiOS allow all traffic on all ports and all IP addresses. Not the most secure. While applying UTM profiles can help to block viruses, detect attacks and prevent spam, this doesn't provide a solid overall security option. The best approach is a layered approach; the first layer being the security policy.

When creating outbound security policies, you need to know the answer to the question "What are the students allowed to do?" The answer is surf the web, connect to FTP sites, send/receive email, and so on.

Once you know what the students need to do, you can research the software used and determine the ports the applications use. For example, if the students only require web surfing, then there are only two ports (80 - HTTP and 443 - HTTPS) needed to complete their tasks. Setting the security policies to only allow traffic through two ports (rather than all 65,000), this will significantly lower any possible exploits. By restricting the ports to known services, means stopping the use of proxy servers, as many of them operate on a non-standard port to hide their traffic from URL filtering or HTTP inspection.

DNS

Students should not be allowed to use whatever DNS they want. this opens another port for them to use and potentially smuggle traffic on. The best approach is to point to an internal DNS server and only allow those devices out on port 53. Its the same approach one would use for SMTP. Only allow the mail server to use port 25 since nothing else should be sending email.

If there is no internal DNS server, then the list of allowed DNS servers they can use should be restrictive. One possible exploit would be for them to set up their own DNS server at home that serves different IPs for known hosts, such as having Google.com sent back the IP for playboy.com.

Encrypted traffic (HTTPS)

Generally speaking, students should not be allowed to access encrypted websites. Encrypted traffic cannot be sniffed, and therefore, cannot be monitored. HTTPS traffic should only be allowed when necessary. Most websites a student needs to access are HTTP, not HTTPS. Due to the nature of HTTPS protocol, and the fact that encryption is an inherent security risk to your network, its use should be restricted.

Adding a security policy that encompasses a list of allowed secure sites will ensure that any HTTPS sites that are required are the only sites a student can go to.

FTP

For the most part, students should not be using FTP. FTP is not HTTP or HTTPS so you cannot use URL filtering to restrict where they go. This can be controlled with destination IPs in the security policy. With a policy that specifically outlines which FTP addresses are allowed, all other will be blocked.

Example security policies

Given these requirements, an example set of security policies could look like the following illustration. In a large setup, all the IPs for the students are treated by one of these four policies.

Simple security policy setup

Seq. No.	ID	Source	Destination	Schedule	Service	Action	Status
1	2	Student PCs	Allowed Websites	always	HTTPS	✓	☑
2	3	Student PCs	all	always	HTTP	✓	☑
3	4	Student PCs	Allowed DNS	always	DNS	✓	☑
4	5	Student PCs	Allowed FTP	always	FTP	✓	☑
5		all	all	always	ANY	⊘	Implicit

The last policy in the list, included by default, is a deny policy.This adds to the potential of error that could end up allowing unwanted traffic to pass. The deny policy ensures that any traffic making it to this point is stopped. It can also help in further troubleshooting by viewing the logs for denied traffic.

With these policies in place, even before packet inspection occurs, the FortiGate, and the network are fairly secure. Should any of the UTM profiles fail, there is still a basic level of security.

UTM security profiles

Antivirus profiles

Antivirus screening should be enabled for any service you have enabled in the security policies. In the case above, HTTP, FTP, as well as POP3 and SMTP (assuming there is email access for students). There is not a virus scan option for HTTPS, because the content is encrypted. Generally speaking, most of the network traffic will be students surfing the web.

To configure antivirus profiles in the web-based manager, go to **Security Profiles > Antivirus**, or use the CLI commands under `config antivirus profile`.

Web filtering

The actual filtering of URLs - sites and content - should be performed by FortiGuard. It is easier and websites are constantly being monitored, and new ones reviewed and added to the FortiGuard databases every day. The FortiGuard categories provide an extensive list of offensive, and non-productive sites.

As well, there are additional settings to include in a web filtering profile to best contain a student's web browsing.

- Web URL filtering should be enabled to set up exemptions for websites that are blocked or reasons other than category filtering. It also prevents the use of IP addresses to get around web filtering.
- Block invalid URLs - HTTPS only. This option inspects the HTTPS certificate and looks at the URL to ensure it's valid. It is common for proxy sites to create an HTTPS certificate with a garbage URL. If the site is legitimate, it should be set up correctly. If the site approach to security is to ignore it, then their security policy puts your network at risk and the site should be blocked.

Web filtering options are configured in the web-based manager by going to **Security Profiles > Web filter**, or in the CLI under `config webfilter profile`.

Advanced options

There are a few Advanced options to consider for a web filtering profile:

- Enable **Provide details for blocked HTTP 4xx and 5xx errors**. Under normal circumstances there are exploits that can be used with 400 and 500 series messages to access the website. While most students probably won't know how to do this, there is no harm in being cautious. It only takes one.
- Enable **Rate Images by URL**. This option only works with Google images. It examines the URL that the images is stored at to get a rating on it, then blocks or allows the image based on the rating of the originating URL. It does not inspect the image contents. Most image search engines to a prefect and pass the images directly to the browser.
- Enable **Block HTTP redirects by rating**. An HTTP redirect is one method of getting around ratings. Go to one website that has an allowed rating, and it redirects to another website that may want blocked.

Categories and Classifications

For the selection of what FortiGuard categories and classifications that should be blocked, that is purely based on the school system and its Internet information policy.

Email Filtering

Other than specific teacher-led email inboxes, there is no reason why a student should be able to access, read or send personal email. Ports for POP3, SMTP and IMAP should not be opened in a security policies.

IPS

The intrusion protection profiles should be used to ensure the student PCs are not vulnerable to attacks, nor do you want students making attacks. As well, IPS can do more than simple vulnerability scans. With a FortiGuard subscription, IPS signatures are pushed to the FortiGate unit. New signatures are released constantly for various intrusions as they are discovered.

FortiOS includes a number of predefined IPS sensors that you can enable by default. Selecting the all_default signature is a good place to start as it includes the major signatures.

To configure IPS sensors in the web-based manager, go to **Security Profiles > Intrusion Protection**, on the CLI use commands under `config ips sensor`.

Application control

Application control uses IPS signatures to limit the use of instant messaging and peer-to-peer applications which can lead to possible infections on a student's PC. FortiOS includes a number of pre-defined application categories. To configure and maintain application control profiles in the web-based manager, go to **Security Profiles > Application Control**. In the CLI use commands under `config application list`.

Some applications to consider include proxies, botnets, toolbars and P2P applications.

Logging

Turn on all logging - every option in this section should be enabled. This is not where you decide what you are going to log. It is simply defining what the UTM profiles can log.

Logging everything is a way to monitor traffic on the network, see what student's are utilizing the most, and locate any potential holes in your security plan. As well, keeping this information may help to prove negligence later in necessary.

Replacement messages list

The replacement message list in **System > Config > Replacement Messages**.

The replacement messages list enables you to view and customize replacement messages. Use the expand arrow beside each type to display the replacement messages for that category. Select the **Edit** icon beside each replacement message to customize that message for your requirements.

Should you make a major error to the code, you can select the **Restore Default** to return to the original message and code base.

If you are viewing the replacement messages list in a VDOM, any messages that have been customized for that VDOM are displayed with a Reset icon that you can use to reset the replacement message to the global version.

For connections requiring authentication, the FortiGate unit uses HTTP to send an authentication disclaimer page for the user to accept before a security policy is in effect. Therefore, the user must initiate HTTP traffic first in order to trigger the authentication disclaimer page. Once the disclaimer is accepted, the user can send whatever traffic is allowed by the security policy.

Replacement message images

You can add images to replacement messages to:

- Disclaimer pages
- Login pages
- Declined disclaimer pages
- Login failed page
- Login challenge pages
- Keepalive pages

Image embedding is also available to the endpoint NAC download portal and recommendation portal replacement messages, as well as HTTP replacement messages.

Supported image formats are GIF, JPEG, TIFF and PNG. The maximum file size supported is 6000 bytes.

Adding images to replacement messages

To upload an image for use in a message

1. Go to **System > Config > Replacement Messages**.
2. Select **Manage Images** at the top of the page.
3. Select **Create New**.
4. Enter a **Name** for the image.
5. Select the **Content Type**.
6. Select **Browse** to locate the file and select **OK**.

The image that you include in a replacement message, must have the following html:

```
<img src=%%IMAGE: <config_image_name>%% size=<bytes> >
```

For example:

```
<img src=%%IMAGE: logo_hq%% size=4272>
```

Modifying replacement messages

Replacement messages can be modified to include a message or content that suits your organization.

Use the expand arrows to view the replacement message list for a given category. Messages are in HTML format. To change a replacement message, go to **System > Config > Replacement Messages** select the replacement message that you want to modify. At the bottom pane of the window, you can see the message on one side and the HTML code on the other side. The message view changes in real-time as you change the content.

A list of common replacement messages appears in the main window. To see the entire list and all categories of replacement messages, in the upper-right corner of the window, select **Extended View**.

Alert Mail replacement messages

The FortiGate unit adds the alert mail replacement messages listed in the following table to alert email messages sent to administrators. If you enable the option **Send alert email for logs based on severity**, whether or not replacement messages are sent by alert email depends on how you set the alert email in **Minimum log level**.

Authentication replacement messages

The FortiGate unit uses the text of the authentication replacement messages for various user authentication HTML pages that are displayed when a user is required to authenticate because a security policy includes at least one identity-based policy that requires firewall users to authenticate.

These replacement message pages are for authentication using HTTP and HTTPS. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

Users see the authentication login page when they use a VPN or a security policy that requires authentication. You can customize this page in the same way as you modify other replacement messages.

There are some unique requirements for these replacement messages:

- The login page must be an HTML page containing a form with `ACTION="/"` and `METHOD="POST"`
- The form must contain the following hidden controls:
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

Example

The following is an example of a simple authentication page that meets the requirements listed above.

```
<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
```

```
      <BODY><H4>You must authenticate to use this service.</H4>
<FORM ACTION="/" method="post">
      <INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">
<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0"
      CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>
<TR><TH>Username:</TH>
      <TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text"> </TD></TR>
<TR><TH>Password:</TH>
      <TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password"> </TD></TR>
<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc">
      <INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden">
          <INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden">
          <INPUT VALUE="Continue" TYPE="submit"> </TD></TR>
</TBODY></TABLE></FORM></BODY></HTML>
```

Captive Portal Default replacement messages

The Captive Portal Default replacement messages are used for wireless authentication only. You must have a VAP interface with the security set as captive portal to trigger these replacement messages.

Device Detection Portal replacement message

The FortiGate unit displays the replacement message when the FortiGate unit cannot determine the type of BYOD or handheld device is used to connect the network.

Email replacement messages

The FortiGate unit sends the mail replacement messages to email clients using IMAP, POP3, or SMTP when an event occurs such as antivirus blocking a file attached to an email that contains a virus. Email replacement messages are text messages.

If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to IMAPS, POP3S, and SMTPS email messages.

Endpoint Control replacement message

The FortiGate unit displays the replacement message when the FortiClient Endpoint Security software is not installed or registered correctly with the FortiGate unit.

FTP replacement messages

The FortiGate unit sends the FTP replacement messages listed in the table below to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session. FTP replacement messages are text messages.

FortiGuard Web Filtering replacement messages

The FortiGate unit sends the FortiGuard Web Filtering replacement messages listed in the table to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection and if **Protocol Recognition > HTTPS Content Filtering Mode** is set to Deep Scan in the antivirus profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

HTTP replacement messages

The FortiGate unit sends the HTTP replacement messages listed in the following table to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the FortiGate unit supports SSL content scanning and inspection, and if under HTTPS in the protocol option list has Enable Deep Scan enabled, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

IM replacement messages

The FortiGate unit sends the IM replacement messages listed in to IM clients using AIM, ICQ, MSN, or Yahoo! Messenger when an event occurs such as antivirus blocking a file attached to an email that contains a virus. IM replacement messages are text messages.

NNTP replacement messages

The FortiGate unit sends the NNTP replacement messages listed in the following table to NNTP clients when an event occurs such as antivirus blocking a file attached to an NNTP message that contains a virus. NNTP replacement messages are text messages.

Spam replacement messages

The FortiGate unit adds the Spam replacement messages listed in the following table to SMTP server responses if the email message is identified as spam and the spam action is discard. If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

NAC quarantine replacement messages

The page that is displayed for the user depends on whether NAC quarantine blocked the user because a virus was found, a DoS sensor detected an attack, an IPS sensor detected an attack, or a DLP rule with action set to **Quarantine IP address** or **Quarantine Interface** matched a session from the user.

The default messages inform the user of why they are seeing this page and recommend they contact the system administrator. You can customize the pages as required, for example to include an email address or other contact information or if applicable a note about how long the user can expect to be blocked.

SSL VPN replacement message

The SSL VPN login replacement message is an HTML replacement message that formats the FortiGate SSL VPN portal login page. You can customize this replacement message according to your organization's needs. The page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with `ACTION="%%SSL_ACT%%"` and `METHOD="%%SSL_METHOD%%"`
- The form must contain the `%%SSL_LOGIN%%` tag to provide the login form.
- The form must contain the `%%SSL_HIDDEN%%` tag.

Web Proxy replacement messages

The FortiGate unit sends Web Proxy replacement messages listed in the table below when a web proxy event occurs that is detected and matches the web proxy configuration. These replacement messages are web pages that appear within your web browser.

The following web proxy replacement messages require an identity-based security policy so that the web proxy is successful. You can also enable FTP-over-HTTP by selecting the **FTP** option in **System > Network > Explicit Proxy**.

Traffic quota control replacement messages

When user traffic is going through the FortiGate unit and it is blocked by traffic shaping quota controls, users see the **Traffic shaper block message** or the **Per IP traffic shaper block message** when they attempt to connect through the FortiGate unit using HTTP.

The traffic quota HTTP pages should contain the `%%QUOTA_INFO%%` tag to display information about the traffic shaping quota setting that is blocking the user.

MM1 replacement messages

MM1 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have **Remove Blocked** selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the FortiGate unit.

MM3 replacement messages

MM3 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have **Remove Blocked** selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the unit.

MM4 replacement messages

MM4 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MM7 replacement messages

MM7 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MMS replacement messages

The MMS replacement message is sent when a section of an MMS message has been replaced because it contains a blocked file. This replacement message is in HTML format.

The message text is:

```
<HTML><BODY>This section of the message has been replaced because it contained a blocked
    file</BODY></HTML>
```

Replacement message groups

Replacement message groups enable you to view common messages in groups for large carriers. Message groups can be configured by going to **Config > Replacement Message Group**.

Using the defined groups, you can manage specific replacement messages from a single location, rather than searching through the entire replacement message list.

If you enable virtual domains (VDOMs) on the FortiGate unit, replacement message groups are configured separately for each virtual domain. Each virtual domain has its own default replacement message group, configured from **System > Config > Replacement Messages Group**.

When you modify a message in a replacement message group, a Reset icon appears beside the message in the group. You can select this Reset icon to reset the message in the replacement message group to the default version.

All MM1/4/7 notification messages for FortiOS Carrier (and MM1 retrieve-conf messages) can contain a SMIL layer and all MM4 notification messages can contain an HTML layer in the message. These layers can be used to brand messages by using logos uploaded to the FortiGate unit via the 'Manage Images' link found on the replacement message group configuration page.

Disk

To view the status and storage information of the local disk on your FortiGate unit, go to **System > Config > Advanced**. The **Disk** menu appears only on FortiGate units with an internal hard or flash disk.

Formatting the disk

The internal disk of the FortiGate unit (if available) can be formatted by going to **System > Config > Advanced** and selecting **Format**.

Formatting the disk will erase all data on it, including databases for antivirus and IPS; logs, quarantine files, and WAN optimization caches. The FortiGate unit requires a reboot once the disk has been formatted.

Setting space quotas

If the FortiGate unit has an internal hard or flash disk, you can allocate the space on the disk for specific logging and archiving, and WAN optimization. By default, the space is used on an as required basis. As such, a disk can fill up with basic disk logging, leaving less potential space for quarantine.

By going to **System > Config > Advanced**, you can select the **Edit** icon for **Logging and Archiving** and **WAN Optimization & Web Cache** and define the amount of space each log, archive and WAN optimization has on the disk.

CLI Scripts

To upload bulk CLI commands and scripts, go to **System > Config > Advanced**.

Scripts are text files containing CLI command sequences. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical security policies, you can enter the commands required to create the security policies in a script, and then deploy the script to all the devices which should use those same settings.

Use a text editor such as Notepad or other application that creates simple text files. Enter the commands in sequence, with each line as one command, similar to examples throughout the FortiOS documentation set.

If you are using a FortiGate unit that is not remotely managed by a FortiManager unit or the FortiGuard Analysis and Management Service, the scripts you upload are executed and discarded. If you want to execute a script more than once, you must keep a copy on your management PC.

If your FortiGate unit is configured to use a FortiManager unit, you can upload your scripts to the FortiManager unit, and run them from any FortiGate unit configured to use the FortiManager unit. If you upload a script directly to a FortiGate unit, it is executed and discarded.

If your FortiGate unit is configured to use FortiGuard Analysis and Management Service, scripts you upload are executed and stored. You can run uploaded scripts from any FortiGate unit configured with your FortiGuard Analysis and Management Service account. The uploaded script files appear on the FortiGuard Analysis and Management Service portal website.

Uploading script files

After you have created a script file, you can then upload it through **System > Config > Advanced**. When a script is uploaded, it is automatically executed.

Commands that require the FortiGate unit to reboot when entered in the command line will also force a reboot if included in a script.

To execute a script

1. Go to **System > Config > Advanced**.
2. Verify that **Upload Bulk CLI Command File** is selected.
3. Select **Browse** to locate the script file.
4. Select **Apply**.

If the FortiGate unit is not configured for remote management, or if it is configured to use a FortiManager unit, uploaded scripts are discarded after execution. Save script files to your management PC if you want to execute them again later.

If the FortiGate unit is configured to use the FortiGuard Analysis and Management Service, the script file is saved to the remote server for later reuse. You can view the script or run it from the FortiGuard Analysis and Management Service portal website.

Rejecting PING requests

The factory default configuration of your FortiGate unit allows the default external interface to respond to ping requests. Depending on the model of your FortiGate unit the actual name of this interface will vary. For the most secure operation, you should change the configuration of the external interface so that it does not respond to ping requests. Not responding to ping requests makes it more difficult for a potential attacker to detect your FortiGate unit from the Internet. One such potential threat are Denial of Service (DoS) attacks.

A FortiGate unit responds to ping requests if ping administrative access is enabled for that interface.

To disable ping administrative access - web-based manager

1. Go to **System > Network > Interface**.
2. Choose the external interface and select **Edit**.

3. Clear the **Ping Administrative Access** check box.
4. Select **OK**.

In the CLI, when setting the allowaccess settings, by selecting the access types and not including the PING option, that option is then not selected. In this example, only HTTPS is selected.

To disable ping administrative access - CLI

```
config system interface
   edit external
      set allowaccess https
end
```

Opening TCP 113

Although seemingly contrary to conventional wisdom of closing ports from hackers, this port, which is used for ident requests, should be opened.

Port 113 initially was used as an authentication port, and later defined as an identification port (see RFC 1413). Some servers may still use this port to help in identifying users or other servers and establish a connection. Because port 113 receives a lot of unsolicited traffic, many routers, including on the FortiGate unit, close this port.

The issue arises in that unsolicited requests are stopped by the FortiGate unit, which will send a response saying that the port is closed. In doing so, it also lets the requesting server know there is a device at the given address, and thus announcing its presence. By enabling traffic on port 113, requests will travel to this port, and will most likely, be ignored and never responded to.

By default, the ident port is closed. To open it, use the following CLI commands:

```
config system interface
   edit <port_name>
      set ident_accept enable
end
```

You could also further use port forwarding to send the traffic to a non-existent IP address and thus never have a response packet sent.

Obfuscate HTTP responses

The FortiGate unit can obfuscate the HTTP responses from the FortiGate admin GUI and SSL VPN servers. By default this option is not enabled. To obfuscate HTTP headers, use the following CLI command:

```
config system global
   set http-obfuscate {none | header-only | modified | no-error}
end
```

Where:

`none` — do not hide the FortiGate web server identity.

`header-only` — hides the HTTP server banner.

`modified` — provides modified error responses.

`no-error` — suppresses error responses.

Chapter 24 - Traffic Shaping

With the ever-increasing demands on network systems for a number of protocols, including email, HTTP traffic both internally and externally to the internet, voice over IP, FTP, and more, slow traffic is becoming a reality. Important traffic may even be dropped or slowed to an unusable speed. Web traffic delays can result in a loss of revenue for businesses.

Traffic shaping attempts to normalize traffic peaks and bursts to prioritize certain flows over others. There is a physical limitation to the amount of data which can be buffered and to the length of time it can be buffered.

FortiGate units provide Quality of Service (QoS) by applying bandwidth limits and prioritization. Using traffic shaping, you can adjust how your FortiGate unit allocates resources to different traffic types to improve performance and stability of latency sensitive or bandwidth intensive network applications.

This chapter describes Quality of Service (QoS), traffic shaping, FortiGate traffic shaping algorithms, and includes configuration procedures for traffic shaping on FortiGate units.

This guide contains the following sections:

The purpose of traffic shaping describes traffic shaping theories and quality of service.

Traffic shaping methods lists different methods of applying traffic shaping within FortiOS, and explains how to use ToS and Differentiated Services.

Examples provides basic application scenarios for shapers.

Troubleshooting traffic shaping lists diagnose commands to use for determining if traffic shapers are working correctly.

The purpose of traffic shaping

Traffic shaping, or traffic management, controls the bandwidth available and sets the priority of traffic processed by the policy to control the volume of traffic for a specific period (bandwidth throttling) or rate the traffic is sent (rate limiting).

Traffic shaping attempts to normalize traffic peaks and bursts to prioritize certain flows over others. But there is a physical limitation to the amount of data which can be buffered and to the length of time. Once these thresholds have been surpassed, frames and packets will be dropped, and sessions will be affected in other ways.

A basic traffic shaping approach is to prioritize certain traffic flows over other traffic whose potential loss is less disadvantageous. This would mean that you accept certain sacrifices in performance and stability on low-priority traffic, to increase or guarantee performance and stability to high-priority traffic.

If, for example, you are applying bandwidth limitations to certain flows, you must accept the fact that these sessions can be limited and therefore negatively impacted.

Note that traffic shaping is effective for normal IP traffic at normal traffic rates. Traffic shaping is not effective during periods when traffic exceeds the capacity of the FortiGate unit. Because packets must be received by the FortiGate unit before they are subject to traffic shaping, if the FortiGate unit cannot process all of the traffic it receives, then dropped packets, delays, and latency are likely to occur.

To ensure that traffic shaping is working at its best, make sure that the interface Ethernet statistics show no errors, collisions or buffer overruns.

Accelerated interfaces (NPx network processors and CE) affect traffic shaping. For more information, see the FortiOS Chapter 12 - Hardware Acceleration guide.

Quality of Service

Quality of Service (QoS) is the capability to adjust some quality aspects of your overall network traffic. This can include such techniques as priority-based queuing and traffic policing. Because bandwidth is finite and because some types of traffic are slow, jitter or packet loss sensitive, bandwidth intensive, or operation critical, QoS can be a useful tool for optimizing the performance of the various applications on your network.

Before implementing QoS, organizations should first identify the types of traffic that are important to the organization, the types of traffic that use high amounts of bandwidth, and the types of traffic that are sensitive to latency or packet loss.

For example, a company might want to guarantee sufficient bandwidth for revenue producing e-commerce traffic. They need to ensure that transactions can be completed and that clients do not experience service delays and interruptions. At the same time, the company may need to ensure low latency for voice over IP (VoIP) traffic used by sales and customer support, while traffic latency and bursts may be less critical to the success of other network applications such as long term, resumable file transfers. Many organizations discover that QoS is especially important for managing their voice and streaming multi-media traffic. These types of traffic can rapidly consume bandwidth and are sensitive to latency.

Discovering the needs and relative importance of each traffic type on your network will help you to design an appropriate overall approach, including how you will configure each available QoS component technique. Some organizations discover that they only need to configure bandwidth limits for some services. Other organizations

determine that they need to fully configure interface and security policy bandwidth limits for all services, and prioritize queuing of critical services relative to traffic rate.

You can implement QoS on FortiGate units using the following techniques:

Traffic policing	Drops packets that do not conform to bandwidth limitations.
Traffic shaping	Ensures that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instant in time. Flows greater than the maximum rate are subject to traffic policing.
Queuing	Transmits packets in order of their assigned priority queue for that physical interface. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.

When deciding how to configure QoS techniques, it can be helpful to know when FortiGate units employ each technique in the overall traffic processing flow, and the considerations that arise from those mechanisms.

Traffic policing

The FortiGate unit begins to process traffic as it arrives (ingress) and departs (egress) on an interface. In later phases of the network processing, such as enforcing maximum bandwidth use on sessions handled by a security policy, if the current rate for the destination interface or traffic regulated by that security policy is too high, the FortiGate unit may drop the packet. Time spent on prior processing, such as web filtering, decryption or IPS, is often wasted on packets that are not forwarded. This applies to VLAN interfaces and physical interfaces.

You can prevent this wasted effort on ingress by configuring the FortiGate unit to preemptively drop excess packets when they are received at the source interface, before most other traffic processing is performed:

```
config system interface
   edit <interface_name>
      set inbandwidth <rate_int>
   next
end
```

where `<rate_int>` is the bandwidth limit in Kb/s. Excess packets will be dropped. If `inbandwidth` is `0`, the rate is not limited.

A similar command is available that can be performed on egress as well using the CLI commands:

```
config system interface
   edit <interface_name>
      set outbandwidth <rate_int>
   next
end
```

As with ingress, setting the rate to 0 (zero) sets the rate to unlimited.

Rate limiting traffic accepted by the interface enables you to restrict incoming traffic to rates that, while no longer the full capacity of the interface, at the traffic shaping point in the processing are more likely to result in acceptable rates of outgoing traffic per destination interface or all security policies. This conserves FortiGate processing resources for those packets that are more likely to be viable completely to the point of egress.

Excessive traffic policing can degrade network performance rather than improve it. For details on factors you may want to consider when configuring traffic policing, see Important considerations on page 2398.

Bandwidth guarantee, limit, and priority interactions

After packet acceptance, the FortiGate unit classifies traffic and may apply traffic policing at additional points during processing. It may also apply additional QoS techniques, such as prioritization and traffic shaping. Traffic shaping consists of a mixture of traffic policing to enforce bandwidth limits, and priority queue adjustment to assist packets in achieving the guaranteed rate.

If you have configured prioritization, the FortiGate unit prioritizes egressing packets by distributing them among FIFO (first in, first out) queues associated with each possible priority number. Each physical interface has six priority queues. Virtual interfaces do not have their own queues, and instead use the priority queues of the physical interface to which they are bound.

Each physical interface's six queues are queue 0 to queue 5, where queue 0 is the highest priority queue. However, for the reasons described below, you may observe that your traffic uses only a subset of those six queues. Some traffic may always use a certain queue number. Some queuing may vary by the packet rate or mixture of services. Some queue numbers may be used only by through traffic for which you have configured traffic shaping in the security policy that applies to that traffic session. For example:

- Administrative access traffic will always use queue 0.
- Traffic matching security policies ***without*** traffic shaping may use queue 0, queue 1, or queue 2. Which queue will be used depends on the priority value you have configured for packets with that ToS (type of service) bit value, if you have configured ToS-based priorities.
- Traffic matching security policies ***with*** traffic shaping may use any queue. Which queue will be used depends on whether the packet rate is currently below the guaranteed bandwidth (queue 0), or above the guaranteed bandwidth. Packets at rates greater than the maximum bandwidth limit are dropped.
- If the global tos-based-priority is low (3), the priority in a traffic-shaper is medium (2) and a packet flows though a policy that refers to the shaper, the packet will be assigned the priority defined by the shaper, in this case medium (2).

Prioritization and traffic shaping behavior varies by your configuration, the service types and traffic volumes, and by whether the traffic is through traffic, or the traffic originates from or terminates at the FortiGate unit itself.

FortiGate traffic

Administrative access to the FortiGate through HTTPS or SSH, or IPsec tunnel negotiations, security policies do not apply, and therefore FortiGate units do not apply traffic shaping. Such traffic also uses the highest priority queue, queue 0. In other words:

packet priority = 0

Exceptions to this rule include traffic types that are connections related to a session governed by a security policy.

For example, if you have enabled scanning by FortiGuard antivirus, traffic from the sender technically terminates at the FortiGate proxy that scans that traffic type; the FortiGate unit initiates a second connection that transmits scanned content to its destination. Because the second connection's traffic is technically originating from the FortiGate proxy and therefore the FortiGate unit itself, it uses the highest priority queue, queue 0. However, this connection is logically associated with through traffic, and is therefore subject to possible bandwidth enforcement and guarantees in its governing security policy. In this way, it behaves partly like other through traffic.

Through traffic

For traffic passing through the FortiGate unit, the method a FortiGate unit uses to determine the priority queue varies by whether Traffic Shaping is enabled or not. Packets may or may not use a priority queue directly or indirectly derived from the type of service (ToS) bit — sometimes used instead with differentiated services — in the packet's IP header.

If Traffic Shaping is not enabled in the security policy, the FortiGate unit neither limits nor guarantees bandwidth, and traffic for that session uses the priority queue determined directly by matching the ToS bit in its header with your configured values:

```
config system global
   set tos-based-priority {high | low | medium}
end
```

or, if you have configured a priority specifically for that ToS bit value:

```
config system tos-based-priority
   edit <id_int>
      set tos [0-15]
      set priority {high | low | medium}
   next
end
```

where `tos` is the value of the ToS bit in the packet's IP header, and `high` has a priority value of 0 and `low` is 2. Priority values configured in the second location will override the global ToS-based priority. In other words:

packet priority = ToS-based priority

For example, you might specify that packets with a ToS bit value of 2 should use queue 0, the highest priority queue:

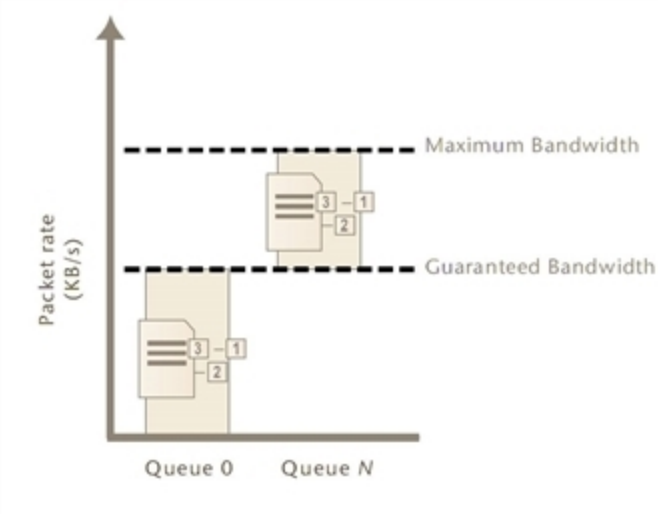
```
config system tos-based-priority
   edit 15
      set tos 2
      set priority high
   next
end
```

If Traffic Shaping is enabled in the security policy using shared traffic shapers, the FortiGate unit may instead or also subject packets to traffic policing, or priority queue increase in an effort to meet bandwidth guarantees configured in the shaper:

```
config firewall shaper traffic-shaper
   edit <shaper_name>
      ...
      set priority {high | medium | low}
      set maximum-bandwidth <rate>
      set guaranteed-bandwidth <rate>
end
```

where `high` has a priority value of 1 and `low` is 3, and `<rate>` is the bandwidth limit in kilobits per second. The diagram below illustrates traffic queuing as the packet rate increases.

Traffic queuing as the packet rate increases



- If the current packet rate is less than Guaranteed Bandwidth, packets use priority queue 0. In other words:

  packet priority = 0
- If the current packet rate is greater than Guaranteed Bandwidth but less than Maximum Bandwidth, the FortiGate unit assigns a priority queue by adding the numerical value of the security policy-based priority, where the value of High is 1, and Low is 3, with the numerical value of the ToS-based priority, where `high` has a priority value of 0 and `low` is 2. Because the two values are added, depending on the your configured ToS-based priorities, packets in this category could use queues from queue 1 to queue 5. In other words:

  packet priority = ToS-based priority + security policy-based priority

  For example, if you have enabled Traffic Shaping in the security policy, and the security policy's Traffic Priority is Low (value 3), and the priority normally applied to packets with that ToS bit is `medium` (value 1), then packets have a total packet priority of 4, and use priority queue 4.
- If the current packet rate exceeds Maximum Bandwidth, excess packets are dropped.

Calculation and regulation of packet rates

Packet rates specified for Maximum Bandwidth or Guaranteed Bandwidth are:

```
rate = amount / time
```

where rate is expressed in kilobits per second (Kb/s).

Burst size at any given instant cannot exceed the amount configured in Maximum Bandwidth. Packets in excess are dropped. Packets deduct from the amount of bandwidth available to subsequent packets and available bandwidth regenerates at a fixed rate. As a result, bandwidth available to a given packet may be less than the configured rate, down to a minimum of 0 Kb/s.

Rate calculation and behavior can alternatively be described using the token bucket metaphor, where:

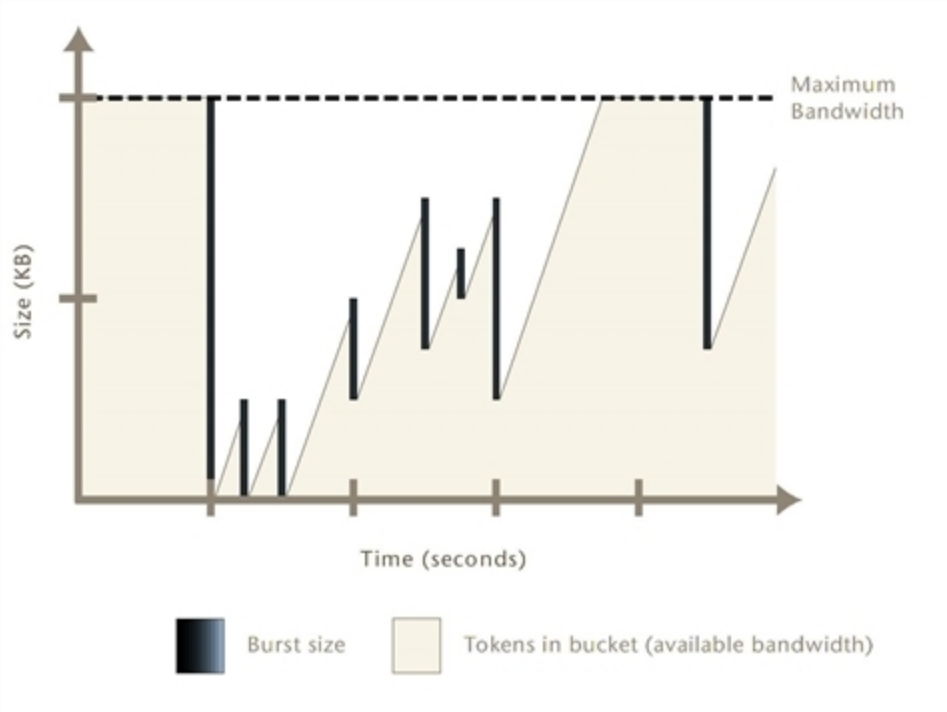
- A traffic flow has an associated bucket, which represents burst size bounds, and is the size of your configured bandwidth limit.
- The bucket receives tokens, which represent available bandwidth, at the fixed configured rate.
- As time passes, tokens are added to the bucket, up to the capacity of the bucket; excess tokens are discarded.

- When a packet arrives, the packet must deduct bandwidth tokens from the bucket equal to its packet size in order to egress.
- Packets cannot egress if there are insufficient tokens to pay for its egress; these nonconforming packets are dropped.

Bursts are not redistributed over a longer interval, so bursts are propagated rather than smoothed, although their peak size is limited.

Maximum burst size is the capacity of the bucket (the configured bandwidth limit); actual size varies by the current number of tokens in the bucket, which may be less than bucket capacity, due to deductions from previous packets and the fixed rate at which tokens accumulate. A depleted bucket refills at the rate of your configured bandwidth limit. Bursts cannot borrow tokens from other time intervals. This behavior is illustrated in the graph below.

Bursts and bandwidth limits over time



By limiting traffic peaks and token regeneration in this way, the available bandwidth at a given moment may be less than bucket capacity, but your limit on the total amount per time interval is ensured. That is, total bandwidth use during each interval of 1 second is at most the integral of your configured rate.

You may observe that external clients, such as FTP or BitTorrent clients, initially report rates between Maximum Bandwidth and twice that of Maximum Bandwidth, depending on the size of their initial burst. This is notably so when a connection is initiated following a period of no network activity.The apparent discrepancy in rates is caused by a difference of perspective when delimiting time intervals. A burst from the client may initially consume all tokens in the bucket, and before the end of 1 second, as the bucket regenerates, be allowed to consume almost another bucket's worth of bandwidth. From the perspective of the client, this constitutes one time interval. From the perspective of the FortiGate unit, however, the bucket cannot accumulate tokens while full; therefore, the time interval for token regeneration begins **after** the initial burst, and does not contain the burst. These different points of reference result in an initial discrepancy equal to the size of the burst — the client's rate contains it, but the FortiGate unit's rate does not. If the connection is sustained to its limit and time progresses

over an increasing number of intervals, however, this discrepancy decreases in importance relative to the bandwidth total, and the client's reported rate will eventually approach that of the FortiGate unit's configured rate limit.

For example, your Maximum Bandwidth might be 50 Kb/s and there has been no network activity for one or more seconds. The bucket is full. A burst from an FTP client immediately consumes 50 Kb. Because the bucket completely regenerates over 1 second, by the time almost another 1 second has elapsed from the initial burst, traffic can consume another 49.999 Kb, for a total of 99.999 Kb between the two points in time. From the vantage point of an external FTP client regulated by this bandwidth limit, it therefore initially appears that the bandwidth limit is 99.999 Kb/s, almost twice the configured limit of 50 Kb/s. However, bucket capacity only regenerates at your configured rate of 50 Kb/s, and so the connection can only consume a maximum of 50 Kb during each second thereafter. The result is that as bandwidth consumption is averaged over an increasing number of time intervals, each of which are limited to 50 Kb/s, the effects of the first interval's doubled bandwidth size diminishes proportionately, and the client's reported rate eventually approaches your configured rate limit. The effects are shown in the table below.

Effects of a 50 Kb/s limit on client reported rates

Total size transferred (Kb)	Time (s)	Rate reported by client (Kb/s)
99.999 (50 + 49.999)	1	99.999
149.999	2	74.999
199.999	3	66.666
249.999	4	62.499
299.999	5	59.998
349.999	6	58.333
…	…	…

Guaranteed Bandwidth can also be described using a token bucket metaphor. However, because this feature attempts to achieve or exceed a rate rather than limit it, the FortiGate unit does not discard non-conforming packets, as it does for Maximum Bandwidth; instead, when the flow does not achieve the rate, the FortiGate unit increases the packets' priority queue, in an effort to increase the rate.

Guaranteed and maximum bandwidth rates apply to the bidirectional total for all sessions controlled by the security policy. For example, an FTP connection may entail two separate connections for the data and control portion of the session; some packets may be reply traffic rather than initiating traffic. All packets for both connections are counted when calculating the packet rate for comparison with the guaranteed and maximum bandwidth rate.

Important considerations

By implementing QoS, you trade some performance and/or stability from traffic X by discarding packets or introducing latency in order to improve performance and stability of traffic Y. The best traffic shaping configuration for your network will balance the needs of each traffic flow by considering not only the needs of your particular organization, but also the resiliency and other characteristics of each particular service.

For example, you may find that web browsing traffic is both more resistant to interruptions or latency and less business critical than UDP or VoIP traffic, and so you might implement less restrictive QoS measures on UDP or VoIP traffic than on HTTP traffic.

An appropriate QoS configuration will also take into account the physical limits of your network devices, and the interactions of the aforementioned QoS mechanisms, described in Bandwidth guarantee, limit, and priority interactions on page 2394.

You may choose to configure QoS differently based upon the hardware limits of your network and FortiGate unit. Traffic shaping may be less beneficial in extremely high-volume situations where traffic exceeds a network interface's or your FortiGate model's overall physical capacity. A FortiGate unit must have enough resources, such as memory and processing power, to process all traffic it receives, and to process it at the required rate; if it does not have this capacity, then dropped packets and increased latency are likely to occur. For example, if the total amount of memory available for queuing on a physical interface is frequently exceeded by your network's typical packet rates, frames and packets must be dropped. In such a situation, you might choose to implement QoS using a higher model FortiGate unit, or to configure an incoming bandwidth limit on each interface.

Incorrect traffic shaping configurations can actually further degrade certain network flows, because excessive discarding of packets or increased latency beyond points that can be gracefully handled by that protocol can create additional overhead at upper layers of the network, which may be attempting to recover from these errors. For example, a configuration might be too restrictive on the bandwidth accepted by an interface, and may therefore drop too many packets, resulting in the inability to complete or maintain a SIP call.

To optimize traffic shaping performance, first ensure that the network interface's Ethernet statistics are clean of errors, collisions, or buffer overruns. To check the interface, enter the following diagnose command to see the traffic statistics:

```
diagnose hardware deviceinfo nic <port_name>
```

If these are not clean, adjust FortiGate unit and settings of routers or other network devices that are connected to the FortiGate unit. For additional information, see Troubleshooting traffic shaping on page 2425.

Once Ethernet statistics are clean, you may want to use only some of the available FortiGate QoS techniques, or configure them differently, based upon the nature of FortiGate QoS mechanisms described in Bandwidth guarantee, limit, and priority interactions on page 2394.

Configuration considerations include:

- For maximum bandwidth limits, ensure that bandwidth limits at the source interface and/or the security policy are not too low, which can cause the FortiGate unit to discard an excessive number of packets.
- For prioritization, consider the ratios of how packets are distributed between available queues, and which queue is used by which types of services. If you assign most packets to the same priority queue, it negates the effects of configuring prioritization. If you assign many high bandwidth services to high priority queues, lower priority queues may be starved for bandwidth and experience increased or indefinite latency. For example, you may want to prioritize a latency-sensitive service such as SIP over a bandwidth-intensive service such as FTP. Consider also that bandwidth guarantees can affect the queue distribution, assigning packets to queue 0 instead of their typical queue in high-volume situations.
- You may or may not want to guarantee bandwidth, because it causes the FortiGate unit to assign packets to queue 0 if the guaranteed packet rate is not currently being met. Comparing queuing behavior for lower-bandwidth and higher-bandwidth situations, this would mean that effects of prioritization only become visible as traffic volumes rise and exceed their guarantees. Because of this, you might want only some services to use bandwidth guarantees, to avoid the possibility that in high-volume situations all traffic uses the same queue, thereby negating the effects of configuring prioritization.

- For prioritization, configure prioritization for all through traffic. You may want to configure prioritization by either ToS-based priority or security policy priority, but not both. This simplifies analysis and troubleshooting.

  Traffic subject to both security policy and ToS-based priorities will use a combined priority from both of those parts of the configuration, while traffic subject to only one of the prioritization methods will use only that priority. If you configure both methods, or if you configure either method for only a subset of your traffic, packets for which a combined priority applies will frequently receive a lower priority queue than packets for which you have only configured one priority method, or for which you have not configured prioritization.

  For example, if both ToS-based priority and security policy priority both dictate that a packet should receive a “medium” priority, in the absence of bandwidth guarantees, a packet will use queue 3, while if only ToS-based priority had been configured, the packet would have used queue 1, and if only security policy-based priority had been configured, the packet would have used queue 2. If no prioritization had been configured at all, the packet would have used queue 0.

For example alternative QoS implementations that illustrate these considerations, see Examples on page 2418.

Traffic shaping methods

In FortiOS, there are three types of traffic shaping configurations. Each has a specific function, and all can be used together in varying configurations. Policy shaping enables you to define the maximum bandwidth and the guaranteed bandwidth set for a security policy. Per-IP shaping enables you to define traffic control on a more granular level. Application traffic shaping goes further, enabling traffic controls on specific applications or application groupings.

This chapter describes the types of traffic shapers and how to configure them in the web-based manager and the CLI.

Traffic shaping options

When configuring traffic shaping for your network, there are three different methods to control the flow of network traffic to ensure that the desired traffic gets through while also limiting the bandwidth that users use for other less important or bandwidth consuming traffic. The three shaping options are:

- Shared policy shaping - bandwidth management by security policies
- Per-IP shaping - bandwidth management by user IP addresses
- Application control shaping - bandwidth management by application

Shared policy shaping and Per-IP shaping are enabled within the security policy under **Policy & Objects** > **Policy**. Application control shaping is enabled under **Security Profiles** > **Application Control**, and setting the **Action** to **Traffic Shaping**.

The three different traffic shaping options offered by the FortiGate unit can also be enabled at the same time within the same security policy. Generally, the hierarchy for traffic shapers in FortiOS is:

- Application Control shaper
- Security policy shaper
- Per-IP shaper

Within this hierarchy, if an application control list has a traffic shaper defined, it will always have precedence over any other security policy shaper. For example, the Facebook application control example shown in Application control shaping on page 2407 will supersede any security policy enabled traffic shapers. While the Facebook application may reach its maximum bandwidth, the user can still have the bandwidth room available from the shared shaper and, if enabled, the per-IP shaper.

Equally, any security policy shared shaper will have precedence over any per-IP shaper. However, traffic that exceeds any of these shapers will be dropped. For example, the policy shaper will take effect first, however, if the per-IP shaper limit is reached first, then traffic for that user will be dropped even if the shared shaper limit for the policy has not been exceeded.

Shared policy shaping

Traffic shaping by security policy enables you to control the maximum and/or guaranteed throughput for a selected security policy. When configuring a shaper, you can select to apply the bandwidth shaping per policy or for all policies. Depending on your selection, the FortiGate unit will apply the shaping rules differently.

Per policy

When selecting a shaper to be **per policy**, the FortiGate unit will apply the shaping rules defined to each security policy individually.

For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four security policies monitoring traffic through the FortiGate unit. Three of these have the shaper enabled. Each security policy has the same maximum bandwidth of 1000 Kb/s.

Per policy traffic shaping is compatible with client/server (active-passive) transparent mode WAN optimization rules. Traffic shaping is ignored for peer-to-peer WAN optimization and for client/server WAN optimization not operating in transparent mode.

All policies

When selecting a shaper to be for all policies -**All Policies using this shaper** - the FortiGate unit applies the shaping rules to all policies using the same shaper. For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four security policies monitoring traffic through the FortiGate unit. All four have the shaper enabled. Each security policy must share the defined 1000 Kb/s, and is set on a first come, first served basis. For example, if policy 1 uses 800 Kb/s, the remaining three must share 200 Kb/s. As policy 1 uses less bandwidth, it is opened up to the other policies to use as required. Once used, any other policies will encounter latency until free bandwidth opens from a policy currently in use.

Maximum and guaranteed bandwidth

The maximum bandwidth instructs the security policy what the largest amount of traffic allowed using the policy. Depending on the service or the users included for the security policy, this number can provide a larger or smaller throughput depending on the priority you set for the shaper.

The **Maximum Bandwidth** can be set to a value of between 1 and 16776000 kbit/s. The Web-Based Manager gives an error if any value outside of this range is used, but in the CLI a value of 0 can be entered. Setting `maximum-bandwidth` to 0 (zero) prevents any traffic from going through the policy.

The guaranteed bandwidth ensures there is a consistent reserved bandwidth available for a given service or user. When setting the guaranteed bandwidth, ensure that the value is significantly less than the bandwidth capacity of the interface, otherwise no other traffic will pass through the interface or very little an potentially causing unwanted latency.

Traffic priority

Select a Traffic Priority of high, medium or low, so the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server that needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

Be sure to enable traffic shaping on all security policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default. Distribute security policies over all three priority queues.

VLAN, VDOM and virtual interfaces

Policy-based traffic shaping does not use queues directly. It shapes the traffic and if the packet is allowed by the security policy, then a priority is assigned. That priority controls what queue the packet will be put in upon egress. VLANs, VDOMs, aggregate ports and other virtual devices do not have queues and as such, traffic is sent directly

to the underlying physical device where it is queued and affected by the physical ports. This is also the case with IPsec connections.

Shared traffic shaper configuration settings

To configure a shared traffic shaper go to **Policy & Objects > Objects > Traffic Shapers** and select the **Create New** "Plus" sign to create a new traffic shaper.

Type	Select **Shared**.
Name	Enter a name for the traffic shaper.
Apply Shaper	When selecting a shaper to be **Per Policy**, the FortiGate unit will apply the shaping rules defined to each security policy individually. For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four security policies monitoring traffic through the FortiGate unit. Three of these have the shaper enabled. Each security policy has the same maximum bandwidth of 1000 Kb/s. Per policy traffic shaping is compatible with client/server (active-passive) transparent mode WAN optimization rules. Traffic shaping is ignored for peer-to-peer WAN optimization and for client/server WAN optimization not operating in transparent mode. When selecting a shaper to be for all policies - **For All Policies Using This Shaper** - the FortiGate unit applies the shaping rules to all policies using the same shaper. For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four security policies monitoring traffic through the FortiGate unit. All four have the shaper enabled. Each security policy must share the defined 1000 Kb/s, and is set on a first come, first served basis. For example, if policy 1 uses 800 Kb/s, the remaining three must share 200 Kb/s. As policy 1 uses less bandwidth, it is opened up to the other policies to use as required. Once used, any other policies will encounter latency until free bandwidth opens from a policy currently in use.
Traffic Priority	Select level of importance **Priority** so the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. If you do not apply any traffic shaping priority, the priority is set to high priority by default.
Maximum Bandwidth	The maximum bandwidth instructs the security policy what the largest amount of traffic allowed using the policy. Depending on the service or the users included for the security policy, this number can provide a larger or smaller throughput depending on the priority you set for the shaper. Setting **Maximum Bandwidth** to 0 (zero) provides unlimited bandwidth.

Guaranteed Bandwidth	The guaranteed bandwidth ensures there is a consistent reserved bandwidth available for a given service or user. When setting the guaranteed bandwidth, ensure that the value is significantly less than the bandwidth capacity of the interface, otherwise no other traffic will pass through the interface or very little and potentially causing unwanted latency. Setting **Guaranteed Bandwidth** to 0 (zero) provides unlimited bandwidth.
DSCP	Enter the number for the DSCP value. You can use the FortiGate Differentiated Services feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network can use these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network to apply different service levels to packets depending on the DSCP value of the packet. For more information, see Differentiated Services.

Example

The following steps creates a Per Policy traffic shaper called “Throughput” with a maximum traffic amount of 720,000 Kb/s, and a guaranteed traffic of 150,000 Kb/s with a high traffic priority.

To create the shared shaper - web-based manager:

1. Go to **Policy & Objects** > Objects > Traffic Shapers and select the Create New “Plus” sign.
2. Set the **Type** to **Shared**.
3. Enter the **Name** `Throughput`.
4. Set the **Apply shaper** field to **Per Policy**.
5. Set the **Traffic Priority** to **High**.
6. Select the **Maximum Bandwidth** check box and enter the value `150000`.
7. Select the **Guaranteed Bandwidth** check box and enter the value `120000`.
8. Select **OK**.

To create the shared shaper - CLI:

```
config firewall shaper traffic-shaper
   edit Throughput
      set per-policy enable
      set maximum-bandwidth 150000
      set guaranteed-bandwidth 120000
      set priority high
   end
```

Per-IP shaping

Traffic shaping by IP enables you to apply traffic shaping to all source IP addresses in the security policy. As well as controlling the maximum bandwidth users of a selected policy, you can also define the maximum number of concurrent sessions.

Per-IP traffic shaping enables you limit the behavior of every member of a policy to avoid one user from using all the available bandwidth - it now is shared within a group equally. Using a per-IP shaper avoids having to create multiple policies for every user you want to apply a shaper to. Per-IP traffic shaping is not supported over NP2 interfaces.

Per-IP traffic shaping configuration settings

To configure per-IP traffic shaping go to **Firewall Policy & Objects > Objects > Traffic Shapers > Per-IP** and select the **Create New "Plus" sign**.

Type	Select **Per-IP**.
Name	Enter a name for the per-IP traffic shaper.
Maximum Bandwidth	The maximum bandwidth instructs the security policy what the largest amount of traffic allowed using the policy. Depending on the service or the users included for the security policy, this number can provide a larger or smaller throughput depending on the priority you set for the shaper. Setting **Maximum Bandwidth** to 0 (zero) provides unlimited bandwidth.
Maximum Concurrent Connections	Enter the maximum allowed concurrent connection.
Forward DSCP **Reverse DSCP**	Enter the number for the DSCP value. You can use the FortiGate Differentiated Services feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network can use these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network to apply different service levels to packets depending on the DSCP value of the packet. For more information, see Differentiated Services.

Example

The following steps create a Per-IP traffic shaper called "Accounting" with a maximum traffic amount of 720,000 Kb/s, and the number of concurrent sessions of 200.

To create the Per-IP shaper - web-based manager:

1. Go to **Policy & Objects** > **Objects** > **Traffic Shapers** and select the **Create New** "Plus" Icon.
2. Set the **Type** to **Per-IP**.
3. Enter the **Name** `Accounting`.
4. Select the **Maximum Bandwidth** checkbox and enter the value `720000`.
5. Select the **Maximum Concurrent Sessions** checkbox and enter the value `200`.
6. Select **OK**.

To create the shared shaper - CLI:

```
config firewall shaper per-ip-shaper
   edit Accounting
```

```
    set max-bandwidth 720000
    set max-concurrent-session 200
  end
```

Adding Per-IP traffic shapers to a security policy

Per-IP traffic shaping is supported by IPv6 security policies. You can add any Per-IP traffic shaper to an IPv6 security policy in the CLI.

Example

The following steps show you how to add an existing Per-IP traffic shaper to an IPv6 security policy. Ensure that you have already created a Per-IP traffic shaper.

To add a Per-IP traffic shaper to an IPv6 security policy - web-based manager:

1. Go to **Policy & Objects** > **Policy** > **IPv6** and click the **Create New** "Plus" icon.
2. Set the **Incoming Interface** to internal.
3. Set the **Source Address** to **All**.
4. Set the **Outgoing interface** to **any**.
5. Set the **Destination address** to **all**.
6. Set the **Schedule** to **Always**.
7. Set the **Service** to **Any**.
8. Set the **Action** to **Accept**.
9. Under **Traffic Shaping** enable **Per-IP Shaper** and select your shaper from the dropdown menu.

To add a Per-IP traffic shaper to an IPv6 security policy- CLI:

```
config firewall policy6
   edit <security_policy_ID_number>
      set per-ip-shaper <per_ip_shaper>
   end
```

Application control shaping

Traffic shaping is also possible for specific applications for both shared and per-IP shaping. Through the **Security Profiles > Application Control** feature, you can configure a specific application's maximum bandwidth. When configuring the application control features, if the application is set to pass, you can set the traffic shaping options. The shapers available are those set up in the **Policy & Objects > Objects > Traffic Shaping** menu.

For more information on configuring application control shapers, see the FortiOS Chapter 21 - Security Profiles Guide.

Example

This example sets the traffic shaping definition for Facebook to a medium priority, a default traffic shaper.

To add traffic shaping for Facebook - web-based manager:

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** "Plus" icon in the upper right corner of the screen to create a new application group, and enter the name `Web`.
3. Select **OK**.
4. In the **Categories** section, click **Social.Media** and select **Traffic Shaping** from the dropdown menu. The **Traffic Shaping Settings** are now displayed below.
5. In the Traffic Shaping Settings section, set **Forward** to medium-priority.
6. Click **Apply**.

To add traffic shaping for Facebook using a Shared Shaper- CLI:

```
config application list
   edit web
      config entries
         edit 1
            set category 23
            set application 17735
            set action pass
            set shaper medium-priority
         end
```

Application Control Per-IP shaping options are not available in the web-based manager, but you can apply Per-IP shapers in the CLI.

To add traffic shaping for Facebook using a Per-IP Shaper- CLI:

```
config application list
   edit web
      config entries
         edit 1
            set category 23
            set application 17735
            set action pass
            set per-ip-shaper {per_ip_shaper_name}
         end
```

Enabling traffic shaping in the security policy

All traffic shapers are enabled within a security policy, including the Application Control shapers. As such, the shapers go into effect after any DoS detection policies, and before any routing or packet scanning occurs.

Traffic shaping is also supported for IPv6 policies.

To enable traffic shaping - web-based manager:

- Go to **Policy & Objects > Policy > IPv4**.
- Click **Create New** or select an existing policy and click **Edit**.

- Navigate to the **Traffic Shaping** section, enable the **Per-IP Shaper** and select an option from the drop down list.
- Select **OK**.

Shapers applied in the security policy affect outbound or traffic to a destination. To affect inbound, or download, traffic, enable both the **Shared Traffic Shaper** and the **Reverse Shaper**. For more information, see Reverse direction traffic shaping on page 2409.

To enable traffic shaping - CLI:

```
config firewall {policy or policy6}
   edit <policy_number>
      ...
      set traffic-shaper <shaper_name>
      set per-ip-shaper <per_ip_shaper_name>
   end
```

Reverse direction traffic shaping

The shaper you select for the security policy (shared shaper) will affect the traffic in the direction defined in the policy. For example, if the source port is port 1 and the destination is port 3, the shaping affects the flow in this direction only, that is, the upload or outbound direction. By selecting **Shared Traffic Shaper Reverse Direction**, you can define the traffic shaper for the policy in the opposite direction, that is, the download or inbound direction. In this example, from port 3 to port 1.

To add a reverse shaper

1. Go to **Policy & Objects > Policy > IPv4**.
2. Click **Create New** or select an existing policy and click **Edit**.
3. Navigate to the **Traffic Shaping** section, enable the **Shared Shaper** and select a shaper from the dropdown list.
4. Enable the **Reverse Shaper** and select a shaper from the dropdown list.
5. Select **OK**.

Setting the reverse direction only

There may be instances where you only need traffic shaping for incoming connections, which is in the “reverse” direction of typical traffic shapers.

To add a reverse shaper - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Traffic Shaping**.
3. Select **Shared Traffic Shaper Reverse Direction** and select the shaper from the list.
4. Select **OK**.

To configure a reverse-only shaper - CLI:

```
config firewall policy
   edit <policy_number>
      ...
      set traffic-shaper-reverse <shaper_name>
   end
```

Type of Service priority

Type of service (ToS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, using criteria of Delay, Throughput, Priority, Reliability, and Cost. Each quality helps gateways determine the best way to route datagrams. A router maintains a ToS value for each route in its routing table. The lowest priority ToS is 0; the highest is 7 when bits 3, 4, and 5 are all set to 1. There are other seldom used or reserved bits that are not listed here.

Together these bits are the ToS variable of the `tos-based-priority` command. The router tries to match the ToS of the datagram to the ToS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero ToS route. Using increased quality may increase the cost of delivery because better performance may consume limited network resources.

Each bit represents the priority as per RFC 1349:

- 1000 - minimize delay
- 0100 - maximize throughput
- 0010 - maximize reliability
- 0001 - minimize monetary cost

The ToS value is set in the CLI using the commands:

```
config system tos-based-priority
   edit <sequence-number>
      set tos [0-15]
      set priority [high | medium | low]
end
```

Where `tos` is the value of the type of service bit in the IP datagram header with a value between 0 and 15, and `priority` is the priority of this type of service priority. These priority levels conform to the firewall traffic shaping priorities, as defined in RFC 1349.

For example, if you want to configure the FortiGate unit so that reliability is the first priority, set the tos value to 4.

```
config system tos-based-priority
   edit 1
      set tos 4
      set priority high
end
```

For a list of ToS values and their DSCP equivalents see ToS and DSCP traffic mapping on page 2415.

Example

```
config system tos-based-priority
   edit 1
      set tos 1
      set priority low
   next
   edit 4
      set tos 4
      set priority medium
   next
   edit 6
      set tos 6
      set priority high
```

```
    next
end
```

ToS in FortiOS

Traffic shaping and ToS follow the following sequence:

- The CLI command `tos-based-priority` acts as a `tos-to-priority` mapping. FortiOS maps the ToS to a priority when it receives a packet.
- Traffic shaping settings adjust the packet's priority according the traffic.
- Deliver the packet based on its priority.

Differentiated Services

Differentiated Services describes a set of end-to-end Quality of Service (QoS) capabilities. End-to-end QoS is the ability of a network to deliver service required by specific network traffic from one end of the network to another. By configuring differentiated services, you configure your network to deliver particular levels of service for different packets based on the QoS specified by each packet.

Differentiated Services (also called DiffServ) is defined by RFC 2474 and 2475 as enhancements to IP networking to enable scalable service discrimination in the IP network without the need for per-flow state and signaling at every hop. Routers that can understand differentiated services sort IP traffic into classes by inspecting the DS field in IPv4 header or the Traffic Class field in the IPv6 header.

You can use the FortiGate Differentiated Services feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network can use these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network to apply different service levels to packets depending on the DSCP value of the packet.

If the differentiated services feature is not enabled, the FortiGate unit treats traffic as if the DSCP value is set to the default (00), and will not change IP packets' DSCP field. DSCP values are also not applied to traffic if the traffic originates from a FortiGate unit itself.

The FortiGate unit applies the DSCP value and IPsec encryption to the differentiated services (formerly ToS) field in the first word of the IP header. The typical first word of an IP header, with the default DSCP value, is 4500:

- 4 for IPv4
- 5 for a length of five words
- 00 for the default DSCP value

You can change the packet's DSCP field for traffic initiating a session (forward) or for reply traffic (reverse) and enable each direction separately and configure it in the security policy.

Changes to DSCP values in a security policy affect new sessions. If traffic must use the new DSCP values immediately, clear all existing sessions.

DSCP is enabled using the CLI command:

```
config firewall policy
   edit <policy_number>
      ...
      set diffserv-forward enable
      set diffservcode-forward <binary_integer>
      set diffserv-reverse enable
      set diffservcode-rev <binary_integer>
```

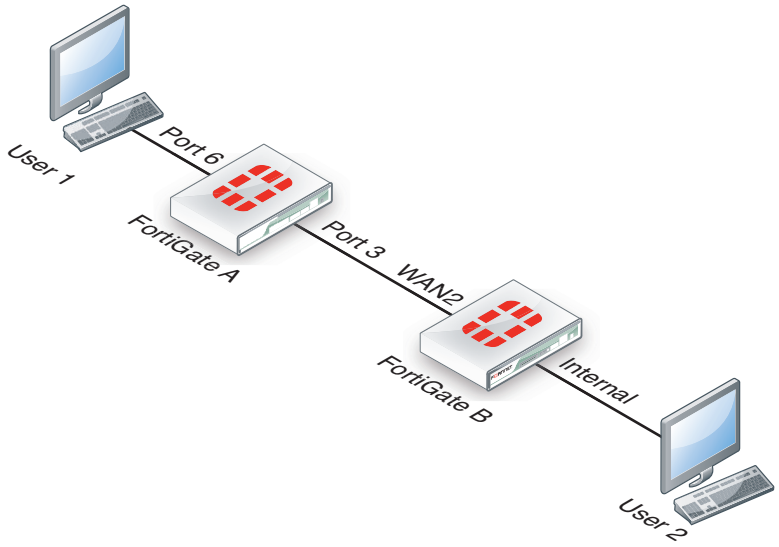
```
end
```

For more information on the different DCSP commands, see the examples below and the CLI Reference. If you only set `diffserv-forward` and `diffserv-reverse` without setting the corresponding `diffvercode` values, the FortiGate unit will reset the bits to zero.

For a list of DSCP values and their ToS equivalents see ToS and DSCP traffic mapping on page 2415. DSCP values can also be defined within a shared shaper as a single value, and per-IP shaper for forward and reverse directions.

DSCP examples

For all the following DSCP examples, the FortiGate and client PC configuration is the following diagram and used firewall-based DSCP configurations.



Example

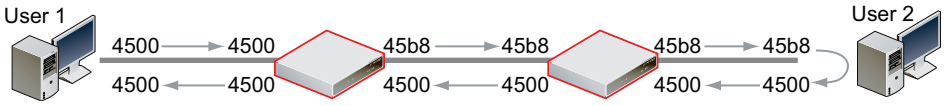
In this example, an ICMP ping is executed between User 1 and FortiGate B, through a FortiGate unit. DSCP is disabled on FortiGate B, and FortiGate A contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf port6
      set dstintf port3
      set src addr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set diffserv-forward enable
      set diffservcode-forward 101110
end
```

As a result, FortiGate A changes the DSCP field for outgoing traffic, but not to its reply traffic. The binary DSCP values used map to the following hexadecimal ToS field values, which are observable by a sniffer (also known as a packet tracer):

- DSCP 000000 is TOS field 0x00
- DSCP 101110 is TOS field 0xb8, the recommended DSCP value for expedited forwarding (EF)

If you performed an ICMP ping between User 1 and User 2, the following output illustrates the IP headers for the request and the reply by sniffers on each of FortiGate unit's network interfaces. The right-most two digits of each IP header are the ToS field, which contains the DSCP value.



Example

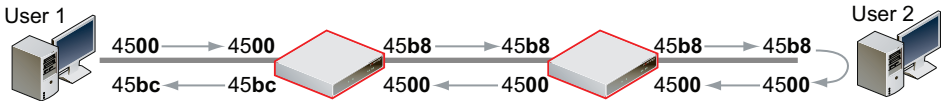
In this example, an ICMP ping is executed between User 1 and FortiGate B, through FortiGate A. DSCP is disabled on FortiGate B, and FortiGate A contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf port6
      set dstintf port3
      set src addr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY"
      set diffserv-forward enable
      set diffserv-rev enable
      set diffservcode-forward 101110
      set diffservcode-rev 101111
   end
```

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic. The binary DSCP values in map to the following hexadecimal ToS field values, which are observable by a sniffer (also known as a packet tracer):

- DSCP 000000 is TOS field 0x**00**
- DSCP 101110 is TOS field 0x**b8**, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field 0x**bc**

If you performed an ICMP ping between User 1 and User 2, the output below illustrates the IP headers observed for the request and the reply by sniffers on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the ToS field, which contains the DSCP value.



Example

In this example, an ICMP ping is executed between User 1 and FortiGate B, through FortiGate A. DSCP is enabled for both traffic directions on FortiGate A, and enabled only for reply traffic on FortiGate B. FortiGate A contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf port6
```

```
      set dstintf port3
      set src addr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set diffserv-forward enable
      set diffserv-rev enable
      set diffservcode-forward 101110
      set diffservcode-rev 101111
   end
```

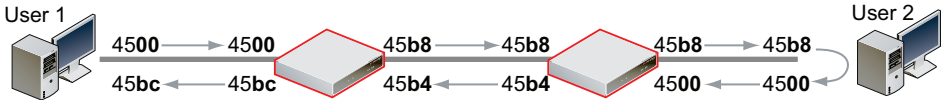
FortiGate B contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf wan2
      set dstintf internal
      set src addr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set diffserv-rev enable
      set diffservcode-rev 101101
   end
```

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic, and FortiGate B changes the DSCP field only for reply traffic. The binary DSCP values in this configuration map to the following hexadecimal ToS field values:

- DSCP 000000 is TOS field 0**x00**
- DSCP 101101 is TOS field 0**xb4**
- DSCP 101110 is TOS field 0**xb8**, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field 0**xbc**

If you performed an ICMP ping between User 1 and User 2, the output below illustrates the IP headers observed for the request and the reply by sniffers on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the ToS field, which contains the DSCP value.



Example

In this example, HTTPS and DNS traffic is sent from User 1 to FortiGate B, through FortiGate A. DSCP is enabled for both traffic directions on FortiGate A, and enabled only for reply traffic on FortiGate B. FortiGate A contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf port6
      set dstintf port3
      set src addr all
      set dstaddr all
```

```
      set action accept
      set schedule always
      set service ANY
      set diffserv-forward enable
      set diffserv-rev enable
      set diffservcode-forward 101110
      set diffservcode-rev 101111
   end
```

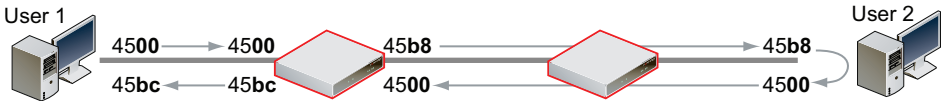
FortiGate B contains the following configuration:

```
config firewall policy
   edit 2
      set srcintf wan2
      set dstintf internal
      set src addr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set diffserv-rev enable
      set diffservcode-rev 101101
   end
```

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic, but FortiGate B changes the DSCP field only for reply traffic which passes through its internal interface. Since the example traffic does not pass through the internal interface, FortiGate B does not mark the packets. The binary DSCP values in this configuration map to the following hexadecimal ToS field values:

- DSCP 000000 is TOS field 0**x00**
- DSCP 101101 is TOS field 0**xb4**, which is configured on FortiGate B but not observed by the sniffer because the example traffic originates from the FortiGate unit itself, and therefore does not match that security policy.
- DSCP 101110 is TOS field 0**xb8**, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field 0**xbc**

If you sent HTTPS or DNS traffic from User 1 to FortiGate B, the following would illustrate the IP headers observed for the request and the reply by sniffers on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the ToS field, which contains the DSCP value.



ToS and DSCP traffic mapping

There are two types of traffic mapping: Type of Service (ToS) or DSCP (Differentiated Services Code Point). Only one method can be used at a time, with ToS set as the default method. You can set the type used and attributes in the CLI.

To set ToS or DSCP traffic mapping

```
config system global
   set traffic-priority {tos | dscp}
   set traffic-priority-level {low | medium | high }
end
```

Mapping of DSCP and ToS hexadecimal values for QoS

Service Class	DSCP Bits	DSCP Value	ToS Value	ToS Hexidecimal
Network Control	111000	56-63	224	0xE0
Internetwork Control	110000	48-55	192	0xC0
Critical - Voice Data (RTP)	101110	46	184	0xB8
	101000	40	160	0xA0
Flash Override Video Data	100010	34	136	0x88
	100100	36	144	0x90
	100110	38	152	0x98
	100000	32	128	0x80
Flash Voice Control	011010	26	104	0x68
	011100	28	112	0x70
	011110	30	120	0x78
	011000	24	96	0x60
Immediate Deterministic (SNA)	010010	18	72	0x48
	010100	20	80	0x50
	010110	22	88	0x58
	010000	16	64	0x40
Priority Controlled Load	001010	10	40	0x28
	001100	12	48	0x30
	001110	14	56	0x38
	001000	8	32	0x20
Routine - Best Effort	000000	0	0	0x00
Routine - Penalty Box	000010	2	8	0x08

Traffic Shaper Monitor

You can view statistical information about traffic shapers and their bandwidth from **Policy & Objects** > **Monitor** > **Traffic Shaper Monitor**.

Refresh	Select to refresh the information on the page.
Reset	Select to reset the information to clear the current information from the page. New information is included on the page.
Report By	Select to display dropped packets or current bandwidth. The chart changes its name so you know what current information is displayed.
Traffic Shaper Usage Dropped packets	The bar chart displays the packets dropped by the traffic shaper.
Traffic Shaper Usage Current Bandwidth	The bar chart displays the current bandwidth of traffic shapers.

Examples

While it is possible to configure QoS using a combination of security policies and in ToSbased priorities, and to distribute traffic over all six of the possible queues for each physical interface, the results of those configurations can be more difficult to analyze due to their complexity. In those cases, prioritization behavior can vary by several factors, including traffic volume, ToS (type of service) or differentiated services markings, and correlation of session to a security policy.

The following simple examples illustrate QoS configurations using either prioritization by security policy, or prioritization by ToS bit, but not both. The examples also assume you are not configuring traffic shaping for interfaces that receive hardware acceleration from network processing units (NPU).

QoS using priority from security policies

Configurations implementing QoS using the priority values defined in the security policies are capable of applying bandwidth limits and guarantees.

In addition to configuring traffic shaping, you may also choose to limit the bandwidth accepted by each interface. This can be useful in scenarios where the bandwidth received on source interfaces frequently exceeds the maximum bandwidth limit defined in the security policy. Rather than waste processing power on packets that will get dropped later in the process, you may choose to preemptively police the traffic.

If you decide to implement QoS using security policies rather than ToS bit, the FortiGate unit applies QoS to all packets controlled by the policy. This type of control is less granular than prioritization by ToS bit, but has the benefits of correlating quality of service to a security policy. This correlation enables you to distribute traffic over up to four of the possible 6 priority queues (queue 0 to queue 3), does not require other devices in your network to set or respect the ToS bit, and enables you to configure bandwidth limits and guarantees.

In the following example, we limit the bandwidth accepted by each source interface, limit the bandwidth used by sessions controlled by the security policy, and then configure prioritized queuing on the destination interface based upon the priority in the security policy, subject to alternative assignment to queue 0 when necessary to achieve the guaranteed packet rate.

To limit bandwidth accepted by an interface

In the CLI, enter the following commands:

```
config system interface
   edit <name_str>
      set inbandwidth <rate_int>
   next
end
```

where `<rate_int>` is the bandwidth limit in Kb/s. Excess packets will be dropped.

To configure bandwidth guarantees, limits, and priorities

1. Go to **Policy & Objects > Objects > Traffic Shapers** and select the Create New “Plus” sign.
2. Select **Shared** or **Per-IP**.
3. Enter a name for the shaper.

4. Enter the **Guaranteed Bandwidth**, if any.
   Bandwidth guarantees affect prioritization. While packet rates are less than this rate, they use priority queue 0. If this is not the effect you intend, consider entering a small guaranteed rate, or enter 0 to effectively disable bandwidth guarantees.
5. Enter a **Maximum Bandwidth**.
   Packets greater than this rate will be discarded.
6. Select the **Traffic Priority**.
   High has a priority value of 1, while Low is 3. While the current packet rate is below Guaranteed Bandwidth, the FortiGate unit will disregard this setting, and instead use priority queue 0.
7. Select **OK**.

Sample configuration

This sample configuration limits ingressing bandwidth to 500 Kb/s. It also applies separate traffic shapers to FTP and HTTP traffic. In addition to the interface bandwidth limit, HTTP traffic is subject to a security policy bandwidth limit of 200 Kb/s.

All egressing FTP traffic greater than 10 Kb/s is subject to a low priority queue (queue 3), while all egressing HTTP traffic greater than 100 Kb/s is subject to a medium priority queue (queue 2). That is, unless FTP traffic rates are lower than their guaranteed rate, and web traffic rates are greater than their guaranteed rate, FTP traffic is lower priority than web traffic.

Traffic less than these guaranteed bandwidth rates use the highest priority queue (queue 0).

Set the inbandwidth limits. This setting is only available in the CLI:

```
config system interface
   edit wan1
      set inbandwidth 500
   next
end
```

Create the traffic shapers for FTP and HTTP.

To configure the FTP and HTTP shapers - web-based manager:

1. Go to **Policy and Objects** > **Objects** > **Traffic Shaper**, and select the **Create New** “Plus” icon.
2. Enter `FTP` for the name of the shaper.
3. Set **Apply Shaper** to **Per policy**.
4. Set the **Traffic Priority** to **Low**.
5. Select the **Guaranteed Bandwidth** checkbox and enter `10` Kbps.
6. Select the **Maximum Bandwidth** checkbox and enter `500` Kbps.
7. Select **OK**.
8. Select the **Create New** “Plus” icon.
9. Enter `HTTP` for the name of the shaper.
10. Select the **Traffic Priority of Medium**.
11. Select the **Guaranteed Bandwidth** checkbox and enter `100` Kbps.
12. Select the **Maximum Bandwidth** checkbox and enter `200` Kbps.
13. Select **OK**.

To configure the FTP and HTTP shapers - CLI:

```
config firewall shaper traffic-shaper
   edit FTP
      set maximum-bandwidth 500
      set guaranteed-bandwidth 10
      set per-policy enable
      set priority low
   next
   edit HTTP
      set maximum-bandwidth 200
      set guaranteed-bandwidth 100
      set per-policy enable
      set priority medium
   end
```

QoS using priority from ToS or differentiated services

Configurations implementing QoS using the priority values defined in either global or specific ToS bit values are not capable of applying bandwidth limits and guarantees, but are capable of prioritizing traffic at per-packet levels, rather than uniformly to all services matched by the security policy.

In addition to configuring traffic prioritization, you may also choose to limit bandwidth being received by each interface. This can sometimes be useful in scenarios where you want to limit traffic levels, but do not want to configure traffic shaping within a security policy. This has the benefit of policing traffic at a point before the FortiGate unit performs most processing.

Note that if you implement QoS using ToS octet rather than security policies, the FortiGate unit applies QoS on a packet by packet basis, and priorities may be different for packets and services controlled by the same security policy. This is more granular control than prioritization by security policies, but has the drawbacks that quality of service is may not be uniform for multiple services controlled by the same security policy, packets will only use up to three of the six possible queues (queue 0 to queue 2), and bandwidth cannot be guaranteed. Other devices in your network must also be able to set or preserve ToS bits.

In this example, we limit the bandwidth accepted by each source interface, and then configure prioritized queuing on the destination interface based upon the value of the ToS bit located in the IP header of each accepted packet.

To limit bandwidth accepted by an interface, in the CLI, enter the following commands:

```
config system interface
   edit <name_str>
      set inbandwidth <rate_int>
   next
end
```

where `<rate_int>` is the bandwidth limit in Kb/s. Excess packets will be dropped.

To configure priorities, in the CLI, configure the global priority value using the following commands:

```
config system global
   set tos-based-priority {high | low | medium}
      end
```

where `high` has a priority value of 0 and `low` is 2.

If you want to prioritize some ToS bit values differently than the global ToS-based priority, configure the priority for packets with that ToS bit value using the following commands:

```
config system tos-based-priority
   edit <id_int>
      set tos [0-15]
      set priority {high | low | medium}
   next
end
```

where and `tos` is the value of the ToS bit in the packet's IP header, and `high` has a priority value of 0 and `low` is 2. Priority values configured in this location will override the global ToS-based priority.

Sample configuration

This sample configuration limits ingressing bandwidth to 500 Kb/s. It also queues egressing traffic based upon the ToS bit in the IP header of ingressing packets.

Unless specified for the packet's ToS bit value, packets use the low priority queue (queue 2). For ToS bit values 4 and 15, the priorities are specified as medium (value 1) and high (value 0), respectively.

```
config system interface
   edit wan1
      set inbandwidth 500
   next
end
config system global
   set tos-based-priority low
end
config system tos-based-priority
   edit 4
      set tos 4
      set priority medium
   next
   edit 15
      set tos 15
      set priority high
   next
end
```

Example setup for VoIP

In this example, there are three traffic shaping requirements for a network:

- Voice over IP (VoIP) requires a guaranteed, high-priority for bandwidth for telephone communications.
- FTP bursts must be contained so as not to consume any available bandwidth. As such this traffic needs to be throttled to a smaller amount.
- A consistent bandwidth requirement is needed for all other email and web-based traffic.

To enable this requirement, you need to create three separate shapers and three security policies for each traffic type.

For this example, the actual values are not actual values, they are used for the simplicity of the example.

Creating the traffic shapers

First create the traffic shapers that define the maximum and guaranteed bandwidth. The shared shapers will be used with some applied per-policy and some applied to all policies, to better control traffic.

VoIP shaper

The VoIP functionary is a key component to the business as a communication tool and as such requires a guaranteed bandwidth.

To create a VoIP shaper - web-based manager:

1. Go to **Policy & Objects** > **Objects** > **Traffic Shapers** and select **Create New**.
2. Set the **Type** to **Shared**.
3. Enter the **Name** `voip`.
4. Select **Per Policy**.
5. Set the **Traffic Priority** to **High**.
6. Select **Maximum Bandwidth** and enter `1000` Kb/s.
7. Select **Guaranteed Bandwidth** and enter `800` Kb/s.
8. Select **OK**.

To create a VoIP shaper - CLI:

```
config firewall shaper traffic-shaper
   edit voip
      set maximum-bandwidth 1000
      set guaranteed-bandwidth 800
      set per-policy enable
      set priority high
   end
```

This ensures that regardless of the number of policies that use this shaper, the defined bandwidth will always be the same. At the same time, the bandwidth is continually guaranteed at 800 Kb/s but if available can be as much as 1000 Kb/s. Setting the priority to high ensures that the FortiGate unit always considers VoIP traffic the most important.

FTP shaper

The FTP shaper sets the maximum bandwidth to use to avoid sudden spikes by sudden uploading or downloading of large files, and interfering with other more important traffic.

To create a FTP shaper - web-based manager:

1. Go to **Policy & Objects** > **Objects** > **Traffic Shapers** and **Create New**.
2. Set the **Type** to **Shared**.
3. Enter the **Name** `ftp`.
4. Set **Apply Shaper** to **All Policies using this shaper**.
5. Set the **Traffic Priority** to **Low**.
6. Select **Maximum Bandwidth** and enter `200` Kb/s

7. Select **Guaranteed Bandwidth** and enter `200` Kb/s.
8. Select **OK**.

To create a FTP shaper - CLI:

```
config firewall shaper traffic-shaper
   edit ftp
      set maximum-bandwidth 200
      set guaranteed-bandwidth 200
      set priority low
   end
```

For this shaper, the maximum and guaranteed bandwidth are set low and to the same value. In this case, the bandwidth is restricted to a specific amount. Setting the traffic priority low ensures that more important traffic will be able to pass before FTP traffic.

Regular traffic shaper

The regular shaper sets the maximum bandwidth and guaranteed bandwidth for everyday business traffic such as web and email traffic.

To create a regular shaper - web-based manager:

1. Go to **Policy & Objects** > **Objects** > **Traffic Shapers** and **Create New**.
2. Set the **Type** to **Shared**.
3. Enter the **Name** `daily_traffic`.
4. Set **Apply Shaper** to **Per Policy**.
5. Set the **Traffic Priority** to **Medium**.
6. Select **Maximum Bandwidth** and enter `600` Kb/s
7. Select **Guaranteed Bandwidth** and enter `600` Kb/s.
8. Select **OK**.

To create a regular shaper - CLI:

```
config firewall shaper traffic-shaper
   edit daily_traffic
      set maximum-bandwidth 600
      set guaranteed-bandwidth 600
      set per-policy enable
      set priority medium
   end
```

For this shaper, the maximum and guaranteed bandwidth are set to a moderate value of 600 Kb/s. It is also set for per policy, which ensures each security policy for day-to-day business traffic has the same distribution of bandwidth.

Creating security policies

To employ the shaper, create security policies that use the shapers within the policies. Create a separate policy for each service and enable traffic shaping. For example, a policy for FTP traffic, a policy for SIP and so on.

For the following steps the VoIP traffic shaper is enabled as well as the reverse direction option. This ensures that return traffic for a VoIP call has the same guaranteed bandwidth as the outgoing call.

To enable traffic shaping in the security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following:

Incoming interface	Internal interface
Source address	All
Outgoing interface	WAN1
Destination address	All
Schedule	always
Service	SIP
Action	ACCEPT

3. Select **Traffic Shaping**.
4. From the drop-down menu, select the voip shaper created in the previous steps.
5. Select **Reverse Direction Traffic Shaping**.
6. Select **OK**.

To enable traffic shaping in the security policy - CLI:

```
config firewall policy
   edit 6
      set srcintf <internal_interface>
      set scraddr all
      set dstintf wan1
      set dstaddr all
      set action accept
      set schedule always
      set service sip
      set traffic-shaper voip
      set reverse-traffic-shaper voip
   end
```

Troubleshooting traffic shaping

This chapter outlines some troubleshooting tips and steps to diagnose the shapers and whether they are working correctly. These diagnose commands include:

- `diagnose sys tos-based-priority`
- `diagnose firewall shaper traffic-shaper`
- `diagnose firewall per-ip-shaper`
- `diagnose debug flow`

Interface diagnosis

To optimize traffic shaping performance, first ensure that the network interface's Ethernet statistics are clean of errors, collisions, or buffer overruns. To check the interface, enter the following diagnose command to see the traffic statistics:

```
diagnose hardware deviceinfo nic <port_name>
```

Shaper diagnose commands

There are specific diagnose commands you can use to verify the configuration and flow of traffic, including packet loss due to the employed shaper.

All of these diagnose troubleshooting commands are supported in both IPv4 and IPv6.

ToS command

Use the following command to list command to view information of the ToS lists and traffic.

```
diagnose sys tos-based-priority
```

This example displays the priority value currently correlated with each possible ToS bit value. Priority values are displayed in order of their corresponding ToS bit values, which can range between 0 and 15, from lowest ToS bit value to highest.

For example, if you have not configured ToS-based priorities, the following appears…

```
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

…reflecting that all packets are currently using the same default priority, high (value 0).

If you have configured a ToS-based priority of `low` (value 2) for packets with a ToS bit value of 3, the following appears…

```
0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0
```

…reflecting that most packets are using the default priority value, except those with a ToS bit value of 3.

Shared shaper

To view information for the shared traffic shaper for security policies enter the command

```
diagnose firewall shaper traffic-shaper list
```

The resultant output displays the information on all available shapers. The more shapers available the longer the list. For example:

```
name Throughput
maximum-bandwidth 1200000 Kb/sec
guaranteed-bandwidth 50000 Kb/sec
current-bandwidth 0 B/sec
priority 1
packets dropped 0
```

Additional commands include:

`diagnose firewall shaper traffic-shaper state` - provides the total number of traffic shapers on the FortiGate unit.

`diagnose firewall shaper traffic-shaper stats` - provides summary statistics on the shapers. Sample output looks like the following:

```
shapers 9 ipv4 0 ipv6 0 drops 0
```

Per-IP shaper

To view information for the per-IP shaper for security policies enter the command

```
diagnose firewall shaper per-ip-shaper list
```

The resultant output displays the information on all available per-IP shapers. The more shapers available the longer the list. For example:

```
name accounting_group
maximum-bandwidth 200000 Kb/sec
maximum-concurrent-session 55
packet dropped 0
```

Additional commands include:

`diagnose firewall shaper per-ip-shaper state` - provides the total number of per-ip shapers on the FortiGate unit.

`diagnose firewall shaper per-ip-shaper stats` - provides summary statistics on the shapers. Sample output looks like the following:

```
memory allocated 3 packet dropped: 0
```

You can also clear the per-ip statistical data to begin a fresh diagnoses using:

```
diagnose firewall shaper per-ip-shaper clear
```

Packet loss with statistics on shapers

For each shaper there are counters that allow to verify if packets have been discarded. To view this information, in the CLI, enter the command diagnose firewall shaper. The results will look similar to the following output:

```
diagnose firewall shaper traffic-shaper list
name limit_GB_25_MB_50_LQ
maximum-bandwidth 50 Kb/sec
guaranteed-bandwidth 25 Kb/sec
current-bandwidth 51 Kb/sec
priority 3
dropped 1291985
```

The diagnose command output is different if the shapers are configured either per-policy or shared between policies.

For per-IP the output would be:

```
diagnose firewall shaper per-ip-shaper list

name accounting_group
maximum-bandwidth 200000 Kb/sec
maximum-concurrent-session 55
packet dropped 3264220
```

Packet lost with the debug flow

When using the debug flow diagnostic command, there is a specific message information that a packet has exceed the shaper limits and therefor discarded:

```
diagnose debug flow show console enable
diagnose debug flow filter addr 10.143.0.5
diagnose debug flow trace start 1000

id=20085 trace_id=11 msg="vd-root received a packet(proto=17, 10.141.0.11:3735-
    >10.143.0.5:5001) from port5."
id=20085 trace_id=11 msg="Find an existing session, id-0000eabc, original direction"
id=20085 trace_id=11 msg="exceeded shaper limit, drop"
```

Session list details with dual traffic shaper

When a Security Policy has a different traffic shaper for each direction, it is reflected in the session list output from the CLI:

```
diagnose sys session list

session info: proto=6 proto_state=02 expire=115 timeout=3600 flags=00000000 sock
flag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=Limit_25Mbps prio=1 guarantee 25600/sec max 204800/sec traffic 48/sec
reply-shaper=Limit_100Mbps prio=1 guarantee 102400/sec max 204800/sec traffic 0/sec
ha_id=0 hakey=44020
policy_dir=0 tunnel=/
state=may_dirty rem os rs
statistic(bits/packets/allow_err): org=96/2/1 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->3/3->2 gwy=10.160.0.1/0.0.0.0
hook=pre dir=org act=dnat 192.168.171.243:2538->192.168.182.110:80(10.160.0.1:80)
hook=post dir=reply act=snat 10.160.0.1:80->192.168.171.243:2538(192.168.182.110:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0 serial=00011e81 tos=ff/ff app=0
    dd_type=0 dd_rule_id=0
```

Additional Information

- Packets discarded by the shaper impact flow-control mechanisms like TCP. For more accurate testing results prefer UDP protocol.
- Traffic shaping accuracy is optimum for security policies without a protection profile where no FortiGate content inspection is processed.

- Do not oversubscribe an outbandwith throughput. For example, sum[guaranteed BW] < outbandwith. For accuracy in bandwidth calculation, it is required to set the “outbandwidth” parameter on the interfaces. For more information see Bandwidth guarantee, limit, and priority interactions on page 2394.
- The FortiGate unit is not prioritizing traffic based on the DSCP marking configured in the security policy. However, ToS based prioritizing can be made at ingress. For more information see Differentiated Services on page 2411.

Chapter 25 - Transparent Mode

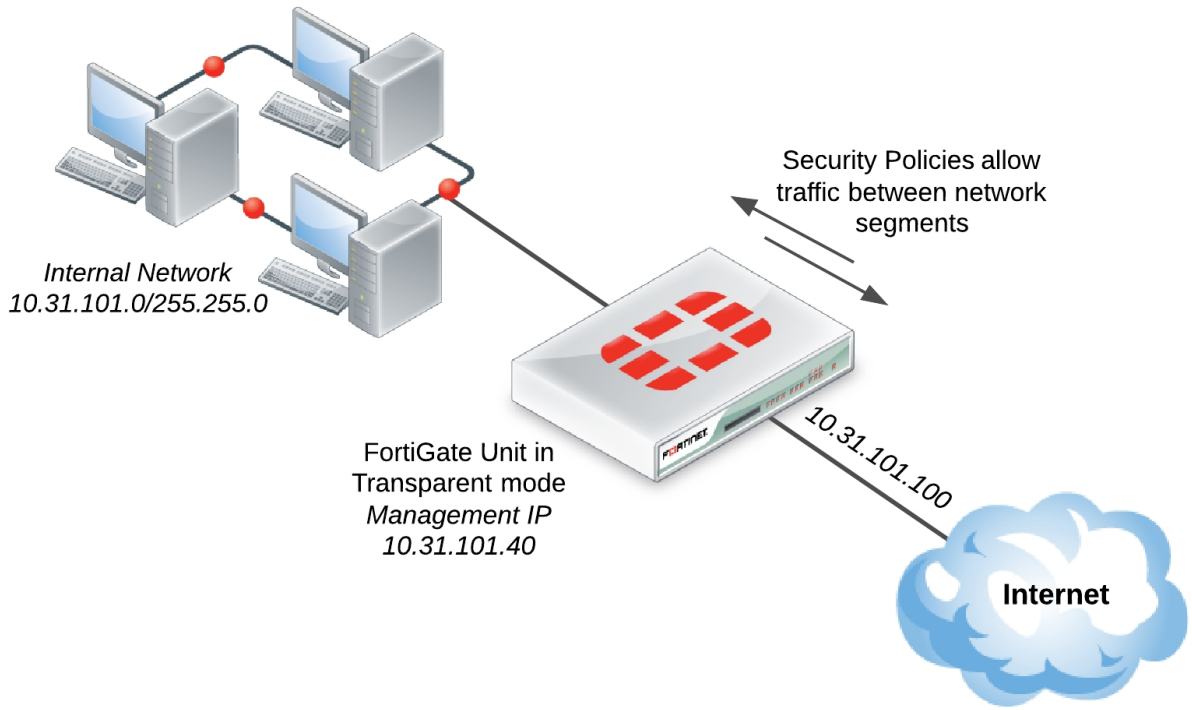
What is Transparent Mode?

A FortiGate unit can operate in one of two modes: Transparent or NAT/Route mode.

In Transparent mode, the FortiGate is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

In NAT/Route mode, a FortiGate unit is installed as a gateway or router between two networks. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT).

A Network with a FortiGate unit in Transparent mode



Feature matrix - Maximum values

FortiGate features and capabilities matrix - NAT vs Transparent mode

Feature/capability	NAT	Transparent	Comment
Unicast Routing / Policy Based routing	YES	NO	
VIP / IP pools / NAT	YES	YES	Configurable from CLI only in transparent mode
Multicast routing	YES	NO - Options available to forward multicast packets	
L2 forwarding	NO	YES	In Transparent mode, other frames than IP can be forwarded but with no UTM processing.
Firewall (packet filtering / NAT / Authentication)	YES	YES	
IPv6 capable	YES	YES	
Traffic shaping - TOS classification	YES	YES	
Hardware acceleration	YES	YES	
IPS	YES	YES	
Anti-Virus	YES	YES	
WEB filtering and Fortiguard WEB filtering	YES	YES	
Mail filtering and Anti-Spam	YES	YES	
Other UTM features (IM/P2P, DLP)	YES	YES	
IPsec gateway	YES	YES - Policy based mode only	
SSL gateway	YES	NO	
High-Availability (HA) - Virtual Cluster	YES	YES	
802.3ad (LACP / port aggregation)	YES	YES	

Feature/capability	NAT	Transparent	Comment
HA port redundancy	YES	YES	FortiGate hardware dependent
802.1q - VLAN trunking	YES	YES	
802.1d - Spanning Tree	NO	NO - option to forward BPDUs	
Logging and reporting (FAMS, syslog or FortiAnalyzer)	YES	YES	
Managed by FortiManager	YES	YES	

Interfaces in Transparent Mode

For a FortiGate in Transparent mode, the maximum number of Interfaces per VDOM is 254. This value includes both physical and virtual interfaces.

For any other maximum values, please consult the Maximum Values Table, available at docs.fortinet.com.

Installation

Installing a FortiGate in Transparent mode

Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

1. Before connecting the FortiGate unit to your network, go to **System > Dashboard > Status** and locate the **System Information** widget. Beside **Operation Mode**, select **Change**.
2. Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network. Select **OK**.
3. Access the web-based manager by browsing to the new management IP.
4. (Optional) The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers. Select **Apply**.
5. If your network uses IPv4 addresses, go to **Policy & Objects > Policy > IPv4** and select **Create New** to add a security policy that allows users on the private network to access the Internet.
   If your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Config > Features**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Handbook.
   Set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to the Internet-facing interface

(typically WAN1). You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.

6. Make sure the **Action** is set to **ACCEPT**. Select **OK**.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the Security Profiles handbook.

7. Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.
   Alternatively, you can also use the CLI command `execute shutdown`.
8. Connect the FortiGate unit between the internal network and the router.
9. Connect the Internet-facing interface to the router's internal interface and connect the internal network to the FortiGate using an internal port (typically port 1).
10. Power on the FortiGate unit. You will experience downtime before the FortiGate unit starts up completely.

Results

Users on the internal network are now able to browse to the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

If a FortiGate unit operating in Transparent mode is installed between your internet network and a server that is providing a network service to the internal network, such as DNS or DHCP, you must add a wan1-to-internal policy to allow the server's response to flow through the FortiGate unit and reach the internal network.

Using Port Pairing to Simplify Transparent Mode

Once you have successfully installed a FortiGate in Transparent mode, you can use port pairing to simplify the configuration.

When you create a port pair, all traffic accepted by one of the paired interfaces can only exit out the other interface. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

Traffic between port-paired interfaces does not check the bridge table and MAC addresses are not learned. Instead traffic received by one interface in a port pair is forwarded out the other (if allowed by a firewall policy). This makes port pairing useful for unusual topologies where MAC addresses do not behave normally. For example, port paring can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

1. Go to *System* > *Network* > *Interfaces*. Select *Create New* > *Port Pair*. Create a port pair that includes both interfaces.
2. Go to *Policy & Objects* > *Policy* > *IPv4*. Create two security policy that allow traffic to flow between the interfaces in the port pair (for example, if you are pairing *wan1* and *Internal*, create a wan1-to-Internal policy and an Internal-to-wan1 policy).

Traffic should now be able to flow between the interfaces in the port pair. You can verify this by going to *Log & Report* > *Traffic Log* > *Forward Traffic*.

Networking

Introduction

Introduce this mess of a section in a way that makes sense!

Packet Forwarding

MAC learning and L2 Forwarding Table

When operating in Transparent mode, a FortiGate behaves like an L2 switch in accordance with 802.1d principles:

- The forwarding database (FDB) is populated with the network devices MAC addresses during a MAC learning process, based on the source addresses seen in the Ethernet frames ingressing a FortiGate port. Static MAC entries can also be configured using the following CLI command:

```
config system mac-address-table
   edit 00:01:02:03:04:05
      set interface "port3"
   next
end
```

  The FDB table can be verified with the following command: `diagnose netlink brctl name host TP.b`

- Ethernet IP frames forwarding is based on known MAC address on each port.
- As Spanning Tree in not running on the FortiGate, a port that comes up goes immediately into forwarding or flooding state. This last state will not occur once unicast MAC addresses are present in the FDB.

If the FortiGate in Transparent mode bridges traffic to a router or host using a virtual MAC for one direction and a different physical MAC for the other direction (for example when VRRP or HSRP protocols are used), it is highly recommended to create a static MAC entry for the virtual MAC. This is to make sure that the virtual MAC address is present in the FDB.

Broadcast, Multicast, and Unicast forwarding

In Transparent mode, IPv4 packets are typically only forwarded by the FortiGate from a port to another port when a firewall policy is matched with action ACCEPT.

Below are exceptions.

- **L2 (IP) Broadcast frames forwarding:**

L2 (IP) means a L2 frame type 0x0800 (IP) or 0x0806 (ARP)

- **ARP:** by default, ARP broadcasts and ARP reply packets are flooded/forwarded on all ports or VLANs belonging to the same forwarding domain, without the need of firewall policies between the ports. This default behavior is necessary to allow the population of the FDB and allow further firewall policy lookup (see section Transparent mode Firewall processing for more details). This option is configurable at the interface settings level with the parameter arpforward (enabled by default).
- **Non-ARP:** To forward non-ARP broadcasts, the following CLI command is used:

```
config system interface
   edit "port2"
      set broadcast-forward enable
   next
end
```

- **L2 (IP) Multicast frames forwarding:** the FortiGate does not forward frames with multicast destination MAC addresses by default. Multicast traffic such as one used by routing protocols or streaming media may need to traverse the FortiGate which should not interfere this communication.

  Fortinet recommends that the FortiGate is set up using Multicast policies. This allows for greater control and predictability on traffic behavior. However Multicast traffic may be forwarded through a Transparent mode device using the multicast-skip-policy setting. This is detailed in the section "Multicast processing" on page 1.
- **L2 (IP) Unicast frames forwarding:** a frame with a unicast destination MAC address is subject to firewall processing before being forwarded (see "Firewall policies" on page 2447 for more details). This does not apply to ARP replies.

Multicast processing

In Transparent mode, a FortiGate does not forward frames with multicast destination MAC addresses by default. If multicast traffic is required, multicast policies are recommended to allow finer control of this traffic.

Forwarding all multicast traffic with policy

Multicast traffic may have to be forwarded through a Transparent mode device using the `multicast-skip-policy`sytem setting. This is the configuration for this solution:

```
config system settings
   set multicast-skip-policy enable
end
```

In that case, no check is performed on sources/destinations/interfaces. A multicast packet received on an interface is flooded unconditionally to all interfaces (except the incoming interface) belonging to the same forwarding domain.

Configuring firewall multicast-policy

The use of `firewall multicast-policy` allows a finer control over the multicast packets. Hereafter are some commented examples. Note that the parameter multicast-skip-policy mentioned above must be left to disabled.

Those policies can only be configured from the CLI.

1- Simple policy

```
config firewall multicast-policy
   edit 1
      set action accept
   next
end
```

In that case, no check is performed on sources/destinations/interfaces. A multicast packet received on an interface is flooded unconditionally to all interfaces (except the incoming interface) belonging to the same forwarding domain.

2- To restrict incoming and outgoing interfaces:

```
config firewall multicast-policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set action accept
   next
end
```

3- To be more restrictive (example to allow RIP2 packets from port1 to port2 and sourced by 10.10.0.10):

```
config firewall multicast-policy
   edit 1
      set srcintf "port1"
      set srcaddr 10.10.0.10 255.255.255.255
      set dstintf "port2"
      set dstaddr 224.0.0.9 255.255.255.255
      set action accept
   next
end
```

4- This policy will allow all 224.0.0.0/255 range (OSPF, RIPv2, DVMPR…) from port1 to port2

```
config firewall multicast-policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set dstaddr 224.0.0.0 255.255.255
      set action accept
   next
end
```

Source MAC addresses in frames sent by or through the FortiGate

When a FortiGate is in Transparent Mode, it does not typically alter the original source and destination address of packets that flow through the unit. Because of this, end devices do not “see” the MAC address of the FortiGate. However, if network address translation (NAT) is enabled by a firewall policy, the source MAC address will be the MAC address of the FortiGate's management interface.

IP packets that are initiated by the FortiGate (remote management, access to FortiGuard server…) are sent in L2 Ethernet frames that have a source MAC address of the interface in the virtual domain (VDOM) with the lowest MAC address. Below is an example with port2 and port3 in the same VDOM, remote access done via port2, but the sniffer trace showing MAC address of port2. The address of port2 is shown in bold.

```
diagnose hardware deviceinfo nic port2
[…]
Current_HWaddr          00:09:0F:85:3F:C4
Permanent_HWaddr        00:09:0F:85:3F:C4

fgt300 (global) # diagnose hardware deviceinfo nic port3
[…]
Current_HWaddr          00:09:0F:85:3F:C5
Permanent_HWaddr        00:09:0F:85:3F:C5


diagnose sniffer packet port3 "port 80" 6
3.774236 port3 -- 192.168.171.165.2619 -> 192.168.182.136.80: syn 3961770249
0x0000   0009 0f85 3fc4 0009 0f09 3204 0800 4500      ....? .... 2...E.
0x0010   0030 8071 4000 7e06 98d7 c0a8 aba5 c0a8      .0.q@.~ ........
0x0020   b688 0a3b 0050 ec23 d109 0000 0000 7002      ...;.P.# ..... p.
0x0030   ffff d7e7 0000 0204 05b4 0101 0402
```

ARP table

In Transparent mode, the Address Resolution Protocol (ARP) table is used in the following situations:

- For IP traffic received or originated by the FortiGate itself, and in destination of the management device or next-hop.
- When IPsec is used, the FortiGate uses its ARP table to forward the traffic from the IPsec tunnel to the local destination host(s).

All other forwarding decision is based on the Forwarding Database (FDB) table or optional settings.

Verifying the forwarding database

To view all instances of the forwarding database (FDB), use the following CLI command:

```
diagnose netlink brctl list
```

Example

```
FGT # diagnose netlink brctl list

list bridge information
1. root.b      fdb: size=256    used=6     num=7     depth=2     simple=no
2. mgmt.b      fdb: size=256    used=5     num=4     depth=2     simple=no
Total 2 bridges
```

Here above we can see two bridge instances for 2 VDOMs in Transparent mode: `root` and `mgmt`.

- This command will dump the L2 forwarding table for each VDOM bridge instance:

```
diagnose netlink brctl name host <VDOM_name>.b
```

Example for the root VDOM:

```
FGT# diag netlink brctl name host root.b

show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
port no device  devname  mac addr                  ttl      atributes
   2     7      wan2     02:09:0f:78:69:00          0        Local Static
   5     6      trunk_1  02:09:0f:78:69:01          0        Local Static
   3     8      dmz      02:09:0f:78:69:01          0        Local Static
   4     9      internal 02:09:0f:78:69:02          0        Local Static
   3     8      dmz      00:80:c8:39:87:5a          194
   4     9      internal 02:09:0f:78:67:68          8
   1     3      wan1     00:09:0f:78:69:fe          0        Local Static
```

Spanning Tree BPDUs forwarding

Spanning tree Bridge Protocol Data Units (BPDUs) are not forwarded by default in Transparent Mode. To forward spanning tree BPDUs, the following setting can be applied on each interface where this is required:

```
config system interface
   edit port1
      set stpforward enable
   next
end
```

Non-IPv4 Ethernet frames forwarding

In the situation where non IP frames (or non Ethernet II) frames need to be accepted on a port, the parameter `l2forward` can be enabled (disabled by default). This can be used to forward frames such as PPPoE PADI, Appletalk, on other ports belonging to the same forwarding domain.

The procedure is the following:

```
config system interface
   edit port1
      set l2forward enable
   next
   edit port2
      set l2forward enable
   next
end
```

NAT

Configuring SNAT

Source Network Address Translation (SNAT) is an option available in Transparent mode and configurable in CLI only, using the following commands:

```
config firewall ippool
   edit "nat-out"
      set endip 192.168.183.48
      set startip 192.168.183.48
      set interface vlan18_p3
   next
end

config firewall policy
   edit 3
      set srcintf "vlan160_p2"
      set dstintf "vlan18_p3"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set ippool enable
      set poolname "nat-out"
      set schedule "always"
      set service "ANY"
      set nat enable
   next
end
```

The sniffer trace below shows the source IP 192.168.182.93 being source translated to 192.168.183.48:

```
fgt300 (TP) # diagnose sniffer packet any "host 10.2.2.1" 4

interfaces=[any]
filters=[host 10.2.2.1]
4.891970 vlan160_p2 in 192.168.182.93 -> 10.2.2.1: icmp: echo request
4.892003 vlan18_p3 out 192.168.183.48 -> 10.2.2.1: icmp: echo request
4.892007 port3 out 192.168.183.48 -> 10.2.2.1: icmp: echo request
4.933216 vlan18_p3 in 10.2.2.1 -> 192.168.183.48: icmp: echo reply
```

```
4.933249 vlan160_p2 out 10.2.2.1 -> 192.168.182.93: icmp: echo reply
4.933253 port2 out 10.2.2.1 -> 192.168.182.93: icmp: echo reply
```

Configuring DNAT

The following example shows how to configure Destination Network Address Translation (DNAT) using a virtual IP on a FortiGatein Transparent Mode:

```
config firewall vip
   edit "vip1"
      set extip 192.168.183.48
      set extintf "vlan160_p2"
      set mappedip 192.168.182.78
   next
end

config firewall policy
   edit 4
      set srcintf "vlan160_p2"
      set dstintf "vlan18_p3"
      set srcaddr "all"
      set dstaddr "vip1"
      set action accept
      set schedule "always"
      set service "ANY"
   next
end
```

If the `mappedip` is on a different subnet than the management IP, the FortiGate must have a valid routeto this destination

The sniffer trace below shows the destination IP 192.168.183.48 being translated to 192.168.182.78:

```
fgt300 (TP) # diagnose sniffer packet any "icmp" 4

interfaces=[any]
filters=[icmp]
4.126138 vlan160_p2 in 192.168.182.93 -> 192.168.183.48: icmp: echo request
4.126190 vlan18_p3 out 192.168.182.93 -> 192.168.182.78: icmp: echo request
4.126196 port3 out 192.168.182.93 -> 192.168.182.78: icmp: echo request
4.126628 vlan18_p3 in 192.168.182.78 -> 192.168.182.93: icmp: echo reply
4.126661 vlan160_p2 out 192.168.183.48 -> 192.168.182.93: icmp: echo reply
4.126667 port2 out 192.168.183.48 -> 192.168.182.93: icmp: echo reply
```

VLANs and Forwarding Domains

Forwarding Domains

A forwarding domain is used to create separate broadcast domains and confine traffic across two or more ports. It also allows learning the same MAC in different VLANs (IVL). See section "VLAN trunking and MAC address learning" on page 2444 for more details.

A forwarding domain and its associated ID number are unique across one VDOM, or a FortiGate with VDOMs disabled. Each new VDOM will create a new bridge instance in the FortiGate.

Even though the forwarding domain ID is not in relation with the actual VLAN numbers, it recommended, for maintenance and troubleshooting purposes, to configure one forwarding domain per VLAN and use the same forwarding domain ID as the VLANs ID.

Once forwarding domains are configured, it is possible to configure firewall policies only between ports or VLAN belonging to the same forwarding domain.

Figure 4 shows an example with three forwarding domains and VLANs configured. In this example, there are two VDOMs in Transparent Mode: root and MGMT. Forwarding domain 0 is the default on the FortiGate or VDOM in Transparent Mode.

- Root VDOM has:
  - 3 forwarding domains, 0, 340, and 341.
  - VLAN 340 configured on port1; packets will be tagged with ID 340
  - VLAN 341 configured on port1; packets will be tagged with ID 341
  - All other ports are untagged
- MGMT VDOM has got only the default forwarding domain 0

The expected behavior is the following:

- Packets untagged ingressing port1, port3 and port4 belong to the same broadcast domain in the root VDOM
- Packets tagged with VLAN 340 ingressing port1 and Packets untagged ingressing port2 belong to the same broadcast domain in the root VDOM
- Packets tagged with VLAN 341 ingressing port1 and Packets untagged ingressing port5 belong to the same broadcast domain in the root VDOM
- Packets untagged ingressing port6 belong to a different broadcast domain in the MGMT VDOM

Configuration example for forwarding domain 340:

```
config system interface
   edit "VLAN340"
      set forward-domain 340
      set interface "port1"
      set vlanid 340
   next
      edit "port3"
         set forward-domain 340
   next
end
```

VLANs in Transparent Mode

A VLAN configured on a physical port is used to classify a packet in a broadcast domain in ingress and to tag packet in egress. A VLAN on the FortiGate conforms to the standard 802.1q. The following rules apply to VLAN configuration:

- a VLAN ID can be used only once on the same physical port
- the same VLAN ID can be used on a different port
- the VLAN ID range is from 1 to 4094

VLANs vs a forwarding domain

There are several differences between VLAN and a forwarding domain configured on a FortiGate in Transparent Mode:

- A forwarding domain is used to create separated broadcast domains between VLANs and allow independent VLAN learning - IVL (MAC addresses in the FDB). This would be equivalent to creating VLANs on a regular L2 switch.

When VLANs are used in the network, configuring different forwarding domains is essential to avoid broadcast duplications. See also section Default VLAN forwarding behavior for additional information.

- VLANs configured on interfaces are only used for tagging packets egressing the port and classifying packets at ingress.
- The packets processed by the direct interface (or port) itself are always sent untagged and must be received untagged.

Default VLAN forwarding behaviour

By default, the parameter **vlanforward** is enabled on each physical interface of a FortiGate or VDOM in Transparent mode.

This allows to forward all VLANs traffic of a trunk that was connecting two network devices and where the FortiGate has been introduced, without having to perform any further configuration.

It is recommended to configure forwarding domains for each VLAN and disable this parameter in order to avoid packet from looping into the trunk from one VLAN to another.

Configuration example:

```
config system interface
   edit port1
      set vlanforward disable
   next
   edit port2
      set vlanforward disable
   next
end
```

Unknown VLAN processing

When a FortiGate receives a tagged frame with an unknown VLAN ID, the processing is the following:

- By default, the ports are set with the parameter `vlanforward enable`; in this scenario, all tagged frames are forwarded to the ports belonging to the same forwarding domain. This allows you to insert the FortiGate between two devices using trunk ports without any further configuration.
- When using forwarding domains in association with VLANs, `vlanforward` should be disabled whenever applicable. In this scenario, any new tagged frames with unknown VLAN IDs are dropped by the FortiGate. This is the solution recommended by Fortinet.

For an example VLAN configuration, see"Configuration example" on page 2446.

VLAN trunking and MAC address learning

A FortiGate port becomes a trunk when 2 or more VLANs are configured on this port, in the same or different forwarding domains.

When trunks are configured on a FortiGate, it is essential to create forwarddomains, in order to avoid packets looping back on the VLANs of the trunk. This will confine all broadcasts and multicast traffic between the interfaces belonging to a same forward domain.

In the case where a trunk port is configured with a VLAN in a different forwarding domains, the MAC address of the network device connected to this port learns the FDB of each forwarding domain. This is Independent VLAN Learning (IVL).

VLAN translation

The same forwarding domain can include several different VLANs. Therefore, a frame ingressing an interface with a certain VLAN ID can be forwarded to another port with another VLAN ID. This is sometimes referred as VLAN translation.

Other

Inter-VDOM links between NAT mode and Transparent mode VDOMs

Inter-VDOM links between NAT and Transparent mode VDOMS can be useful for configurations where the NAT based VDOMs that share a common Internet service route, which can be routed through a Transparent VDOM that provides additional functionality, like common Security inspection, WAN optimization, explicit proxying and so on.

Other examples include:

- Performing SSL offloading in the Transparent mode VDOM and providing Internet access through a NAT mode VDOM.
- Applying WAN optimization in a Transparent mode VDOM and other security features in the NAT mode VDOM.
- Using a dedicated Transparent mode VDOM for the explicit web proxy in front of a NAT mode VDOM that applies other security features.
- An ISP configuration with multiple per-tenant NAT mode VDOMs all sharing a single Internet connection but where the ISP only presents a single routed subnet. Each tenant can then be assigned an IP from the subnet for their respective VDOM link interface while using a single physical port to connect to the ISP router.

For more information about inter-VDOM links, please refer to the Virtual Domains handbook.

Packet forwarding using Cisco protocols

In order to pass Cisco Discover Protocol (CDP) or Cisco VLAN Trunk Protocol (VTP) packets through a FortiGate in Transparent mode, the parameter `stpforward` must be applied on the port configuration. VTP and CDP packets are sent to the destination MAC address 01-00-0C-CC-CC-CC

A Cisco NATIVE VLAN carries CDP/VTP frames. The frames of this VLAN must be received on the FortiGate physical interfaces (not VLAN sub-interface). Physical interfaces are the only ones that can send/accept non-tagged packets.

The example below will allow CDP and VTP packets to be sent from port3 up to the Remote unit, through two VDOMs, via one physical port and three port aggregations.

Port and Port aggregation configuration:

```
config system interface
   edit "port1"
      set vdom "VD1"
   next
   edit "port2"
      set vdom "VD1"
   next
   edit "port3"
      set vdom "VD1"
      set stpforward enable
   next
   edit "port5"
      set vdom "VD3"
   next
   edit "port6"
      set vdom "VD3"
   next
   edit "port17"
      set vdom "VD2"
   next
   edit "port18"
      set vdom "VD2"
   next
   edit "port19"
      set vdom "VD2"
   next
   edit "port20"
      set vdom "VD2"
   next
   edit "LACP_VD2_IN"
      set vdom "VD2"
      set stpforward enable
      set type aggregate
         set member "port17" "port18"
   next
   edit "LACP_VD2_OUT"
      set vdom "VD2"
      set stpforward enable
      set type aggregate
         set member "port19" "port20"
   next
   edit "LACP_VD1"
      set vdom "VD1"
      set stpforward enable
      set type aggregate
         set member "port1" "port2"
   next
end
```

- When using aggregation, the `stpforward` setting needs to be applied only on the port aggregation level, not on the physical port
- This will also forward regular Spanning Tree BPDUs

Verification with a sniffer trace:

```
FGT# diagnose sniffer packet any "" 4

41.365434 port3 in llc unnumbered, ui, flags [command], length 72
41.365437 LACP_VD1 out llc unnumbered, ui, flags [command], length 72
41.365439 port2 out llc unnumbered, ui, flags [command], length 72
41.365479 LACP_VD2_IN in llc unnumbered, ui, flags [command], length 72
41.365482 LACP_VD2_OUT out llc unnumbered, ui, flags [command], length 72
41.365484 port19 out llc unnumbered, ui, flags [command], length 72
```

See above the CDP packet flow from port3, LACP_VD1 (port2), LACP_VD2_IN, LACP_VD2_OUT (port19)

The following sniffer trace command will filter only CDP or VTP packets :

```
FGT# diagnose sniffer packet port_name "ether host 01-00-
0C-CC-CC-CC"
```

Configuration example

Step 1: Create VLANs and forwarding domains

```
config system interface
   edit "vlan102_intern"
   set forward-domain 102
   set interface "port2"
   set vlanid 102
next
   edit "vlan102_extern"
   set forward-domain 102
   set interface "port3"
   set vlanid 102
next
   edit "vlan103_intern"
   set forward-domain 103
   set interface "port2"
   set vlanid 103
next
   edit "vlan103_extern"
   set forward-domain 103
   set interface "port3"
   set vlanid 103
next
end
```

Step 2: Create the appropriate Firewall Policies

```
config firewall policy
   edit 1
      set srcintf "vlan102_extern"
```

```
        set dstintf "vlan102_intern"
           set srcaddr "all"
           set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY" next
     edit 2
        set srcintf "vlan102_intern"
        set dstintf "vlan102_extern"
           set srcaddr "all"
           set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY" next
     edit 3
        set srcintf "vlan103_intern"
        set dstintf "vlan103_extern"
           set srcaddr "all"
           set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY" next
     edit 4
        set srcintf "vlan103_extern"
        set dstintf "vlan103_intern"
           set srcaddr "all"
           set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY" next
  end
```

Firewall policies

Firewall policy look up

In Transparent mode, like in NAT mode, a firewall policy look up is based on the source and destination interfaces. The matching firewall policy will tell which actions to apply to the traffic, including logging and security scanning.

The FortiGate proceeds as follows to look for a matching firewall policy in Transparent mode:

- **Step 1:** an Ethernet IP frame ingresses a port (or a VLAN on a port), corresponding to a specific bridge instance (from the port VDOM and Forwarding domain). This frame contains a destination MAC address that we will call MAC_D.
- **Step 2:** The FortiGate is making a MAC_D address lookup in the bridge instance to determine the port where MAC_D has been learned. This will be the destination interface.
- **Step 3:** The FortiGate is then looking for a firewall policy corresponding to the couple < source interface + destination interface >. If multiple policies with the same couple < source interface + destination interface > exist, the FortiGate screens all of them from TOP to BOTTOM (as displayed in the configuration), until a match is found. It is important to make sure that the most specific firewall policies are located at the top of the policy list, to make sure that traffic is matched to the appropriate policy.

Security scanning

Security scanning occurs in the same manner in NAT mode and Transparent mode. When a protection profile is enabled on a firewall policy for content inspection, the FortiGate acts like a transparent proxy for the protocols that need to be inspected.

The FortiGate will therefore intercept the TCP sessions and create its own session from client to server and server to client. The source and destination MAC addresses of the original L2 frames are however not altered in this communication, as described in the section Network operation : source MAC addresses in frames sent by or through the FortiGate.

Devices in the network communicating through the FortiGate do not know the presence of the FortiGate.

For more information about security scanning, see the Security Profileshandbook.

Firewall session list

The flag **br** in the state line will indicate that this is a “bridged” session. See example below :

```
FGT# diagnose sys session list

session info: proto=17 proto_state=00 duration=59 expire=128 timeout=0 flags=000
00000 sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 hakey=0
policy_dir=0 tunnel=/
state=may_dirty br rem
statistic(bytes/packets/allow_err): org=385/5/1 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.182.93:1025->4.2.2.1:53(0.0.0.0:0)
hook=post dir=reply act=noop 4.2.2.1:53->192.168.182.93:1025(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1 serial=000006d3 tos=ff/ff
imp2p=0 app=0
dd_type=0 dd_rule_id=0
```

ISF ACL policies

Traffic accepted and forwarded by an ISF policy is not subject to security inspection. Normally, you should only create ISF policies for traffic that you consider very low risk.

On FortiGate models that include NP4 and XLR ports and an integrated switch fabric , you can create an integrated switch fabric (ISF) access control list (ACL) firewall policy that allows some traffic (for example, multicast traffic) to bypass security inspection, resulting in reduced CPN and NP4 processor load.

This feature is only available in Transparent mode and only between port pairs.

Use the following command to add an ISF ACL shortcut policy:

```
config firewall isf-acl
   config port-pair-1
      edit 1
         set type binary
         set ingressport {port1 | port2}
         set offset
         set length
         set matchpattern <pattern in hex>
         set action {bypass | block}
      next
      edit 2
         set type 5-tuple
         set srcaddr: a.b.c.d/32
         set dstaddr 239.A.A.a/32
         set proto UDP
         set port XXX
         set action {bypass | block}
      end
   end
```

FortiGate remote management

Management IP configuration in Transparent mode

A FortiGate in Transparent mode can be assigned with a single IP address for remote access management and multiple static routes can be configured. This can be used if in-band management wants to be applied.

When out-of-band management is desired (dedicated interface for remote management access), it is recommended to use a separate VDOM in NAT mode.

In-band management details and example

The management IP address is bound to all ports or VLANs belonging to the same VDOM. Remote access services are subject to the same rules as in NAT mode, and must be enabled/disabled on each port.

Example of management IP configuration in Transparent mode:

```
config system settings
   set manageip 10.1.1.100/255.255.255.0
end
config router static
   edit 1
      set gateway 10.1.1.254
   next
end
config system interface
   edit port1
      set allowaccess ping ssh https snmp
end
```

It is also possible to add a second IP address for management and additional default routes:

```
config system settings
   set opmode transparent
   set manageip 192.168.182.136/255.255.254.0 10.1.1.1/255.255.255.0
end

config router static
   edit 1
      set gateway 192.168.183.254
   next
   edit 2
      set gateway 10.1.1.254
   next
end
```

`ping-server` (dead gateway detection) is not supported in Transparent mode.

Out-of-band management details and example

When VDOM is enabled and the VDOMs are operating in Transparent mode, it is recommended, to avoid L2 loops and allow more routing flexibility, to keep one VDOM (generally the root VDOM) in NAT mode, with one or more VLAN or physical interface as out-of-band management.

The management VDOM must have IP connectivity to the Internet to allow communication with the FDS and retrieve services information (AV,IPS, Fortiguard filtering, Support…). All syslog and FortiManager communication also go through the management VDOM.

FortiManager, FortiAnalyzer

FortiManager, logging and reporting and FortiAnalyzer are supported similarly to NAT mode. For more information about this please consult the Fortinet documentation at http://docs.fortinet.com or the Knowledge base at http://kb.fortinet.com.

Establishing a secured IPSec communication to a FortiAnalyzer is done as per the example hereafter (from global level if VDOM is enabled). This setting is independent from being in Transparent mode. However, as stated earlier in this section the management VDOM must have IP connectivity to the FortiAnalyzer.

```
FGT (global) # show system fortianalyzer

config system fortianalyzer
   set status enable
   set server 10.2.2.2
   set encrypt enable
   set psksecret fortinet
end
```

Transparent mode and HA

Transparent mode and HA

For complete information about HA, please refer to the Fortigate Administration Guide or the HA Technical guides available at http://docs.fortinet.com or the Knowledge Base at http://kb.fortinet.com.

Any other statement and feature description in this document apply to a FortiGate Cluster running in Active-Passive mode.

HA MAC address assignment

If a cluster is operating in Transparent mode, the FortiGate Clustering Protocol (FGCP) assigns a virtual MAC address for the Master unit management IP address. Since you can connect to the management IP address from any interface, all of the FortiGate interfaces appear to have the same virtual MAC address.

Virtual cluster

If VDOM (virtual domain) is enabled on a cluster operating Transparent Mode, HA Virtual Clustering can be configured in active-passive mode.

This will provide:

- Failover protection between two instances of a VDOM operating on two different FortiGate in the cluster.
- Load balancing between the FortiGate units on a per-VDOM basis.

The roles have been defined such as, in normal operation:

- FortiGate1 is Master for Vdom1 and Slave for Vdom2
- FortiGate2 is Master for Vdom2 and Slave for Vdom1

In case of a failure or reboot of a FortiGate, the remaining unit will become Master for Vdom1 and Vdom2.

The VDOMs given in this example are showing physical ports but a VDOM can also include VLAN interfaces.

The L2 connectivity between the FortiGate is showing 4 separate L2 switches, but it could also be one single switch one each side configured with appropriate VLANs.

Configuration example

- FortiGate1:

```
FGT1 (global) # show system ha
```

```
config system ha
   set mode a-p
   set hbdev "port5" 0 "port6" 0
   set vcluster2 enable
   set override disable
   set priority 200
      config secondary-vcluster
         set override enable
         set priority 100
         set vdom "Vdom2"
      end
end
```

- FortiGate2:

```
FGT2 (global) # show system ha

config system ha
   set mode a-p
   set hbdev "port5" 0 "port6" 0
   set vcluster2 enable
   set override disable
   set priority 200
      config secondary-vcluster
         set override enable
         set priority 100
         set vdom "Vdom2"
      end
end
```

IPsec VPN in Transparent mode

Rules and details

In Transparent mode, IPsec VPN is supported in Policy-based configuration mode only.

IPsec VPN in Transparent mode can be used in those scenarios:

- Encrypt data over routed networks without changing anything on the routers. See example 1.
- Encrypt data over a non-routed transport network (extension of a LAN for example). See example 2.

The following rules apply to IPsec in Transparent mode:

- If both remote FortiGate IPsec gateways are not in the same broadcast domain (separated by routers):
  - The hosts on each side must be on different subnets.
  - The FortiGate management IP addresses must be in the same subnet as the local hosts. This is the preferred option.
- If both remote FortiGate IPsec gateways are in the same broadcast domain (separated by optical switches for examples), the hosts on each side can be :
  - On the same subnet
  - On different subnet if the appropriate static route is configured on the remote Fortigate
  - The FortiGate management IP addresses can be in any different subnet than the local hosts

- A firewall Policy with the action IPsec is used to send traffic to the remote device into the tunnel. Therefore, it is important to place all remote devices on the appropriate ports of the Fortigate to allow a proper match < source interface + destination interface > . See section Transparent mode Firewall processing for more details.

This scenario requires that the remote hosts located on the remote FortiGate's protected subnets have their MAC addresses hardcoded in FortiGate's static MAC entry list. If this is not configured then it is expected to see outage in network communications.

Example 1 - remote sites in different subnets

This example provides a configuration example for IPsec VPN tunnels between three FortiGate in Transparent Mode in different subnets, as well as some troubleshooting steps.

The expectation for this example is that PC1 will be able to communicate via the IPsec tunnels with PC2 and PC3, which are in different subnets.

The requirements for this example are:

- Because both FortiGate are not in the same broadcast domain (separated by routers), the hosts on each side must be on different subnets.
- FortiGate management IP addresses must be in the same subnet as the local hosts
- The default gateways (router1 ,router2, router3) for PC1 , PC2 and PC3 must be behind port2 in order for the FortiGate to match the appropriate Encrypt firewall policy (port1 --> port2)

Configuration of FortiGate 1 (FGT1):

Only relevant parts of configuration are provided.

```
config system settings
   set opmode transparent
   set manageip 10.1.1.100/255.255.255.0
end

config router static
   edit 1
      set gateway 10.1.1.254
   next
end

config firewall address
   edit "10.1.1.0/24"
      set subnet 10.1.1.0 255.255.255.0
   next
   edit "10.2.2.0/24"
      set subnet 10.2.2.0 255.255.255.0
   next
   edit "10.3.3.0/24"
      set subnet 10.3.3.0 255.255.255.0
   next
end

config vpn ipsec phase1
   edit "to_FGT2"
```

```
      set proposal 3des-sha1 aes128-sha1 des-md5
      set remote-gw 10.2.2.100
      set psksecret fortinet
   next
   edit "to_FGT3"
      set proposal 3des-sha1 aes128-sha1 des-md5
      set remote-gw 10.3.3.100
      set psksecret fortinet
   next
end

config vpn ipsec phase2
   edit "to_FGT2"
      set keepalive enable
      set phase1name "to_FGT2"
      set proposal 3des-sha1 aes128-sha1
      set dst-subnet 10.2.2.0 255.255.255.0
      set src-subnet 10.1.1.0 255.255.255.0
   next
   edit "to_FGT3"
      set keepalive enable
      set phase1name "to_FGT3"
      set proposal 3des-sha1 aes128-sha1
      set dst-subnet 10.3.3.0 255.255.255.0
      set src-subnet 10.1.1.0 255.255.255.0
   next
end

config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.1.1.0/24"
      set dstaddr "10.2.2.0/24"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT2"
   next
   edit 3
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.1.1.0/24"
      set dstaddr "10.3.3.0/24"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT3"
   next
end
```

Configuration of FortiGate 2 (FGT2):

Only relevant parts of configuration are provided.

```
config system settings
   set opmode transparent
   set manageip 10.2.2.100/255.255.255.0
end

config router static
   edit 1
      set gateway 10.2.2.254
   next
end

config firewall address
   edit "10.1.1.0/24"
      set subnet 10.1.1.0 255.255.255.0
   next
   edit "10.2.2.0/24"
      set subnet 10.2.2.0 255.255.255.0
   next
end

config vpn ipsec phase1
   edit "to_FGT1"
      set nattraversal disable
      set proposal 3des-sha1 aes128-sha1 des-md5
      set remote-gw 10.1.1.100
      set psksecret fortinet
   next
end

config vpn ipsec phase2
   edit "to_FGT1"
      set keepalive enable
      set phase1name "to_FGT1"
      set proposal 3des-sha1 aes128-sha1
      set dst-subnet 10.1.1.0 255.255.255.0
      set src-subnet 10.2.2.0 255.255.255.0
   next
end

config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.2.2.0/24"
      set dstaddr "10.1.1.0/24"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT1"
   next
end
```

Troubleshooting procedure

All steps given when PC1 pings PC2.

Verify if IPsec tunnels are up

```
FGT1 # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=to_FGT2 ver=0 serial=1 10.1.1.100:0->10.2.2.100:0 lgwy=dyn tun=tunnel mode= auto
bound_if=0
proxyid_num=1  child_num=0  refcnt=7  ilast=0  olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=1455
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_FGT2 proto=0 sa=0 ref=1 auto_negotiate=0 serial=5
   src: 10.1.1.0/255.255.255.0:0
   dst: 10.2.2.0/255.255.255.0:0
```

The above tunnel is down (output given as example)!

```
FGT2 # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=to_FGT1 10.2.2.100:0->10.1.1.100:0 lgwy=dyn tun=tunnel mode=auto bound_if=0
proxyid_num=1 child_num=0 refcnt=7 ilast=1 olast=1
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=21 natt:
mode=none draft=0 interval=0 remote_port=0
proxyid=to_FGT1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
   src: 10.2.2.0/255.255.255.0:0
   dst: 10.1.1.0/255.255.255.0:0
   SA: ref=3 options=00000009 type=00 soft=0 mtu=1436 expire=1771 replaywin=0 seq no=1
   life: type=01 bytes=0/0 timeout=1773/1800
   dec: spi=c1a8e951 esp=3des key=24 9213fdf22b150e01abb3535d1a647044eebf772b92f2f7ee
   ah=sha1 key=20 66a38bf99f0b2d234f64b5a05187995c4f56f6bb
   enc: spi=322067b4 esp=3des key=24 720e5680329937fb3630b7ed70bd41bb3114d3c269ae8b61
   ah=sha1 key=20 e316113eb6ea03b014b3a5f9c1a3bd386637801a
```

The above tunnel is up!

Verify that destination local hosts are seen in the ARP table (necessary for IPsec despite being in TP mode)

```
FGT2 # get system arp

Address     Age(min)  Hardware Addr       Interface
10.2.2.10   2         00:50:56:00:76:04   root.b
10.2.2.254  0         00:09:0f:30:29:e4   root.b
```

Using the debug flow command on the initiator side (example on FortiGate1)

```
FGT1 # diagnose debug flow filter addr 10.1.1.10
FGT1 # diagnose debug flow show console enable
FGT1 # diagnose debug enable
FGT1 # diagnose debug flow trace start 50

FGT1 # id=36870 trace_id=615 msg="vd-root received a packet(proto=1, 10.1.1.10:512-
>10.2.2.10:8) from port1."
id=36870 trace_id=615 msg="allocate a new session-00000636"
id=36870 trace_id=615 msg="Allowed by Policy-1: encrypt"
id=36870 trace_id=615 msg="enter IPsec tunnel-to_FGT2"
id=36870 trace_id=615 msg="SA is not ready yet, drop"
id=36870 trace_id=616 msg="vd-root received a packet(proto=1, 10.1.1.10:512->10.2.2.10:8)
    from port1."
id=36870 trace_id=616 msg="Find an existing session, id-00000636, original direction"
id=36870 trace_id=616 msg="enter IPsec tunnel-to_FGT2"
id=36870 trace_id=616 msg="encrypted, and send to 10.2.2.100 with source 10.1.1.100"
id=36870 trace_id=616 msg="send out via dev-port2, dst-mac-00:09:0f:30:29:e0"
id=36870 trace_id=617 msg="vd-root received a packet(proto=1, 10.1.1.10:512->10.2.2.10:8)
    from port1."
id=36870 trace_id=617 msg="Find an existing session, id-00000636, original direction"
id=36870 trace_id=617 msg="enter IPsec tunnel-to_FGT2"
id=36870 trace_id=617 msg="encrypted, and send to 10.2.2.100 with source 10.1.1.100"
id=36870 trace_id=617 msg="send out via dev-port2, dst-mac-00:09:0f:30:29:e0"
id=36870 trace_id=618 msg="vd-root received a packet(proto=1, 10.2.2.10:512->10.1.1.10:0)
    from port2."
id=36870 trace_id=618 msg="Find an existing session, id-00000636, reply direction"
id=36870 trace_id=618 msg="send out via dev-port1, dst-mac-00:50:56:00:76:03"
id=36870 trace_id=619 msg="vd-root received a packet(proto=1, 10.1.1.10:512->10.2.2.10:8)
    from port1."
id=36870 trace_id=619 msg="Find an existing session, id-00000636, original direction"
id=36870 trace_id=619 msg="enter IPsec tunnel-to_FGT2"
id=36870 trace_id=619 msg="encrypted, and send to 10.2.2.100 with source 10.1.1.100"
id=36870 trace_id=619 msg="send out via dev-port2, dst-mac-00:09:0f:30:29:e0"
id=36870 trace_id=620 msg="vd-root received a packet(proto=1, 10.2.2.10:512->10.1.1.10:0)
    from port2."
id=36870 trace_id=620 msg="Find an existing session, id-00000636, reply direction"
id=36870 trace_id=620 msg="send out via dev-port1, dst-mac-00:50:56:00:76:03"
```

The message "`id=36870 trace_id=615 msg="SA is not ready yet, drop`" simply means that the tunnel was not up yet.

Using the debug flow command on the receiver side (example on FortiGate2)

```
FGT2 # diagnose debug flow filter addr 10.1.1.10
FGT2 # diagnose debug flow show console enable
FGT2 # diagnose debug enable
FGT2 # diagnose debug flow trace start 50

FGT2 # id=36870 trace_id=51 msg="vd-root received a packet(proto=1, 10.1.1.10:512-
    >10.2.2.10:8) from port2."
id=36870 trace_id=51 msg="allocate a new session-00000435"
id=36870 trace_id=51 msg="Allowed by Policy-1:"
```

```
id=36870 trace_id=51 msg="send out via dev-port1, dst-mac-00:50:56:00:76:04"
id=36870 trace_id=52 msg="vd-root received a packet(proto=1, 10.2.2.10:512->10.1.1.10:0)
    from port1."
id=36870 trace_id=52 msg="Find an existing session, id-00000435, reply direction"
id=36870 trace_id=52 msg="enter IPsec tunnel-to_FGT1"
id=36870 trace_id=52 msg="encrypted, and send to 10.1.1.100 with source 10.2.2.100"
id=36870 trace_id=52 msg="send out via dev-port2, dst-mac-00:09:0f:30:29:e4"
```

Using the sniffer trace (example on FortiGate2)

```
FGT2 # diagnose sniffer packet any "host 10.2.2.10" 4

9.460021 root.b out arp who-has 10.2.2.10 tell 10.2.2.100
9.460028 port2 out arp who-has 10.2.2.10 tell 10.2.2.100
9.460034 port1 out arp who-has 10.2.2.10 tell 10.2.2.100
9.460462 port1 in arp reply 10.2.2.10 is-at 0:50:56:0:76:4
9.460462 root.b in arp reply 10.2.2.10 is-at 0:50:56:0:76:4
[...]
49.477368 port2 in 10.1.1.10 -> 10.2.2.10: icmp: echo request
49.477444 port1 out 10.1.1.10 -> 10.2.2.10: icmp: echo request
49.477898 port1 in 10.2.2.10 -> 10.1.1.10: icmp: echo reply
50.510023 port2 in 10.1.1.10 -> 10.2.2.10: icmp: echo request
50.510079 port1 out 10.1.1.10 -> 10.2.2.10: icmp: echo request
50.510524 port1 in 10.2.2.10 -> 10.1.1.10: icmp: echo reply
```

The above ARP process in Transparent mode with IPsec is allowing the Fortigate to:

- Identify the MAC address of the destination device 10.2.2.10
- Populate the MAC table (see below), which in turn will give a destination interface and allow a Firewall policy look-up

Check the FDB entries for the destination

```
FGT2 # diagnose netlink brctl name host root.b

port no   device  devname  mac addr            ttl
[..]
1         2       port1    00:50:56:00:76:04    0
```

Example 2 - remote sites in the same subnet and one remote subnet

This example provides a configuration example for IPsec VPN tunnels between two FortiGate in Transparent Mode in the same subnet separated by a L2 transparent network and one remote subnet on the second site.

This scenario requires that PC1's MAC address is added to the FortiGate's static MAC table. The preferred scenario would be to have a router installed between the 2 FortiGate's.

The expectation for this example is that PC1 will be able to communicate via the IPsec tunnel with Server1 in the same subnet, and Server2 in a different subnet.

The requirements for this example are:

- The default gateway (FGT3) for PC1 and all remote device must be behind port2 of FGT1, in order for this FortiGate to match the appropriate Encrypt firewall policy (port1 --> port2)
- Despite being in Transparent mode, **FGT2 must have a valid route to Server2**
- FGT3 is used as a router between subnet 10.1.1.0/24 and 10.3.3.0/24.

PC1 MAC address added to FGT2 static MAC entries.

Server1 MAC address added to FGT1 static MAC entries.

Configuration of FortiGate 1 (FGT1):

Only relevant parts of configuration are provided.

```
config system settings
   set opmode transparent
   set manageip 10.1.1.100/255.255.255.0
end

config router static
   edit 1
      set gateway 10.1.1.252
   next
end

config system mac-address-table
   edit 00:50:56:00:76:04 ==>Server1
      set interface port2
   next
end

config firewall address
   edit "all"
   next
   edit "Server1"
      set subnet 10.1.1.20 255.255.255.255
   next
   edit "Server2"
      set subnet 10.3.3.30 255.255.255.255
   next
   edit "10.1.1.0/24"
      set subnet 10.1.1.0 255.255.255.0
   next
   edit "gateway"
      set subnet 10.1.1.254 255.255.255.255
   next
end

config vpn ipsec phase1
   edit "to_FGT2"
      set proposal 3des-sha1 aes128-sha1 des-md5
      set remote-gw 10.1.1.200
      set psksecret fortinet
   next
end

config vpn ipsec phase2
   edit "to_FGT2"
```

```
      set keepalive enable
      set phase1name "to_FGT2"
      set proposal 3des-sha1 aes128-sha1
      set src-subnet 10.1.1.0 255.255.255.0
   next
end

config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.1.1.0/24"
      set dstaddr "Server1"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT2"
   next
   edit 2
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.1.1.0/24"
      set dstaddr "Server2"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT2"
   next
   edit 3
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "10.1.1.0/24"
      set dstaddr "gateway"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "to_FGT2"
   next
end
```

Firewall Policy 3 is not mandatory and is only used to allow PC1 to test a ping reach-ability to its default gateway 10.1.1.254.

Configuration of FortiGate 2 (FGT2):

Only relevant parts of configuration are provided.

```
config system settings
   set opmode transparent
   set manageip 10.1.1.200/255.255.255.0
end

config router static
   edit 1
      set gateway 10.1.1.252
   next
   edit 2
      set dst 10.3.3.0 255.255.255.0
      set gateway 10.1.1.254
   next
end

config system mac-address-table
   edit 00:50:56:00:76:03
      set interface wan1
   next
end

config firewall address
   edit "all"
   next
   edit "PC1"
      set subnet 10.1.1.10 255.255.255.255
   next
   edit "10.1.1.0/24"
      set subnet 10.1.1.0 255.255.255.0
   next
   edit "10.3.3.0/24"
      set subnet 10.3.3.0 255.255.255.0
   next
end

config vpn ipsec phase1
   edit "to_FGT1"
      set proposal 3des-sha1 aes128-sha1 des-md5
      set remote-gw 10.1.1.100
      set psksecret fortinet
   next
end

config vpn ipsec phase2
   edit "to_FGT1"
      set keepalive enable
      set phase1name "to_FGT1"
      set proposal 3des-sha1 aes128-sha1
      set dst-subnet 10.1.1.0 255.255.255.0
   next
end

config firewall policy
   edit 1
      set srcintf "internal"
      set dstintf "wan1"
      set srcaddr "10.1.1.0/24" set dstaddr "PC1"
```

```
      set action ipsec
      set schedule "always"
      set service "ANY" set inbound enable
      set outbound enable
      set vpntunnel "to_FGT1"
   next
   edit 2
      set srcintf "internal"
      set dstintf "wan1"
      set srcaddr "10.3.3.0/24" set dstaddr "PC1"
      set action ipsec
      set schedule "always"
      set service "ANY" set inbound enable
      set outbound enable
      set vpntunnel "to_FGT1"
   next
end
```

Troubleshooting procedure

Check the ARP entries of PC1

```
C:\ arp -a

Interface: 10.1.1.10 --- 0x20003
Internet Address        Physical Address       Type
10.1.1.20               00-50-56-00-76-04      dynamic
10.1.1.254              00-09-0f-85-3f-c8      dynamic
```

MAC address **00-09-0f-85-3f-c8** is the FGT3 interface in subnet 10.1.1.0/24.

FDB entries of FGT1

```
FGT1 (global) # diagnose netlink brctl name host Vdom1.b

show bridge control interface Vdom1.b host. fdb:
size=256, used=6, num=6, depth=1
Bridge Vdom1.b host table
port no  device devname  mac addr           ttl   attributes
1        10     port1    00:50:56:00:76:03  0
2        9      port2    00:50:56:00:76:04  44    static
2        9      port2    00:09:0f:85:3f:c8  13
1        10     port1    00:09:0f:88:2f:69  0     Local Static
2        9      port2    00:09:0f:88:2f:68  0     Local Static
2        9      port2    00:09:0f:23:01:d6  0
```

MAC address **00:09:0f:23:01:d6** is “internal” port MAC address of FGT2 00:09:0F:23:01:D6. This is the MAC address used for management in the Transparent mode VDOM of FGT2, chosen between the lowest MAC address between wan1 (00:09:0F:78:00:74) and internal (00:09:0F:23:01:D6).

ARP entries of FGT2

```
FGT2 (TP) # get system arp

Address      Age(min)   Hardware Addr         Interface
10.1.1.20    82         00:50:56:00:76:04     TP.b
10.1.1.100   13         00:09:0f:88:2f:68     TP.b
10.1.1.254   76         00:09:0f:85:3f:c8     TP.b
```

it is important to have the entry for 10.1.1.254 which is the route to 10.3.3.0/24 .

IPsec Tunnel verification on FGT1

```
FGT1 (Vdom1) # diagnose vpn tunnel list

list all ipsec tunnel in vd 3
------------------------------------------------------
name=to_FGT2 10.1.1.100:0->10.1.1.200:0 lgwy=dyn tun=tunnel mode=auto bound_if=0
proxyid_num=1 child_num=0 refcnt=10 ilast=0 olast=0
stat: rxp=2754 txp=2945 rxb=308448 txb=176700
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=166 natt:
mode=none draft=0 interval=0 remote_port=0
proxyid=to_FGT2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
   src: 10.1.1.0/255.255.255.0:0
   dst: 0.0.0.0/0.0.0.0:0
   SA: ref=3 options=00000009 type=00 soft=0 mtu=1436 expire=1271 replaywin=0 seqno=1e1
       life:type=01 bytes=0/0 timeout=1750/1800
   dec: spi=3f148cb7 esp=3des key=24 834832201a0dbbf60b0098106f08380538dbd94cacd1ad31
       ah=sha1 key=20 b0257a135cba745b956bef3d4b8a6e65934c074b
   enc: spi=1895305e esp=3des key=24 4d3092f0b3f84184d4779f85a9953230bf9bc28bd93c0afa
       ah=sha1 key=20 0c70acf6ad2193ec5934e2a4332fd09f32016e60
   npu_flag=00 npu_rgwy=10.1.1.200 npu_lgwy=10.1.1.100 npu_selid=0
```

Sniffer trace on FGT1 when PC1 pings all 3 remote destinations

```
FGT1 (Vdom1) # diagnose sniffer packet any "icmp" 4

interfaces=[any]
filters=[icmp]
0.342268 port1 in 10.1.1.10 -> 10.3.3.30: icmp: echo request
0.342844 port2 in 10.3.3.30 -> 10.1.1.10: icmp: echo reply
0.342884 port1 out 10.3.3.30 -> 10.1.1.10: icmp: echo reply
0.771700 port1 in 10.1.1.10 -> 10.1.1.20: icmp: echo request
0.772504 port2 in 10.1.1.20 -> 10.1.1.10: icmp: echo reply
0.772539 port1 out 10.1.1.20 -> 10.1.1.10: icmp: echo reply
0.907377 port1 in 10.1.1.10 -> 10.1.1.254: icmp: echo request
0.907850 port2 in 10.1.1.254 -> 10.1.1.10: icmp: echo reply
0.907883 port1 out 10.1.1.254 -> 10.1.1.10: icmp: echo reply
```

Sniffer trace on FGT1 filtered on IPsec protocol

```
FGT1 (Vdom1) # diagnose sniffer packet port2 "proto 50" 6

interfaces=[port2]
```

```
filters=[proto 50]
pcap_lookupnet: port2: no IPv4 address assigned

1.249003 port2 -- 10.1.1.100 -> 10.1.1.200: ip-proto-50 92
0x0000   0009 0f23 01d6 0009 0f88 2f68 0800 4500     ...# ..... /h..E.
0x0010   0070 c9e6 0000 3f32 9a48 0a01 0164 0a01     .p ... ?2.H...d..
0x0020   01c8 1895 305f 0000 01e2 02b6 37b6 8b2c     ....0_ ..... 7..,

1.249478 port2 -- 10.1.1.200 -> 10.1.1.100: ip-proto-50 92
0x0000   0009 0f88 2f68 0009 0f23 01d6 0800 4500     ..../h...# ... E.
0x0010   0070 2e31 0000 3f32 35fe 0a01 01c8 0a01     .p.1..?25 ......
0x0020   0164 3f14 8cb8 0000 01e2 324d 66e2 9236     .d? ...... 2Mf..6
```

From the above trace, the MAC address **0009 0f88 2f68** is the MAC address of FGT1 port2 . This is the MAC address used for management in the Transparent mode VDOM of FGT1, chosen between the lowest MAC address between port1 (00:09:0F:88:2F:69) and port2 ((00:09:0F:88:2F:68).

Debug flow on FGT1 filtered on Server3

```
FGT1 (Vdom1) # diagnose debug flow filter addr 10.3.3.30
FGT1 (Vdom1) # diagnose debug flow show console enable
FGT1 (Vdom1) # diagnose debug enable
FGT1 (Vdom1) # diagnose debug flow trace start 10

id=20085 trace_id=11 msg="vd-Vdom1 received a packet(proto=1, 10.1.1.10:512->10.3.3.30:8)
    from port1."
id=20085 trace_id=11 msg="Find an existing session, id-00004e85, original direction"
id=20085 trace_id=11 msg="enter IPsec tunnel-to_FGT2"
id=20085 trace_id=11 msg="encrypted, and send to 10.1.1.200 with source 10.1.1.100"
id=20085 trace_id=11 msg="send out via dev-port2, dst-mac-00:09:0f:23:01:d6"
id=20085 trace_id=12 msg="vd-Vdom1 received a packet(proto=1, 10.3.3.30:512->10.1.1.10:0)
    from port2."
id=20085 trace_id=12 msg="Find an existing session, id-00004e85, reply direction"
id=20085 trace_id=12 msg="send out via dev-port1, dst-mac-00:50:56:00:76:03"
```

From the trace above, **dst-mac-00:09:0f:23:01:d6** is “internal” port MAC address of FGT2 00:09:0F:23:01:D6. This is the MAC address used for management in the Transparent mode VDOM of FGT2, chosen between the lowest MAC address between wan1 (00:09:0F:78:00:74) and internal (00:09:0F:23:01:D6).

Replay traffic scenario

Replay traffic scenario

Situations can arise where an identical TCP packet enters twice the FortiGate via 2 different ports. This can be due to a firewall or other network device redirecting packets out on the same port it has received it.

The FortiGate will in this condition detect a replay packet and drop it.

If the network topology or culprit devices cannot be changed to avoid this, the workaround on the FortiGate can be to disable TCP replay verification packets.

```
config system global
   set anti-replay | loose | strict | disable |
end
```

In v3.0 this command was:

```
config system global
   set conn-tracking disable
end
```

*

The debug flow diagnosis output hereafter shows the message indicating this condition:

```
   id=20085 trace_id=179 msg="vd-VDOM_VLAN1 received a packet(proto=6, 10.10.253.9:10709
   >10.10.248.5:25) from TO_EXTERNAL ."
   id=20085 trace_id=179 msg="Find an existing session, id-00041475, original direction"
*  id=20085 trace_id=179 msg="replay packet, drop"
```

For additional diagnosis and troubleshooting procedures, please consult the Knowledge Base at http://kb.fortinet.com.

Transparent mode reminder and best practices

1. Create forwarding domains when VLANs are used and set `vlanforward` to `disable` on all relevant physical interface.
2. The forward-domain ID can be different to the VLAN ID, but it is recommended for troubleshooting and readability to keep them the same.
3. Only interfaces from the same forwarding domains can have firewall policies between each others.
4. In order to allow IVL (independent VLAN learning), the VLANs must be placed in separate forwarding domains.
5. If an out-of-band management is desired, use if possible a VDOM in NAT mode as management VDOM and create (an) other Transparent mode VDOM(s) for the user traffic.
6. As Spanning Tree BPDUs are not forwarded by default, insert the FortiGate with caution to avoid L2 loops.
7. Multicast packets are not forwarded by default; this might cause routing protocols (RIP2,OSPF) disruption.

8. When using HSRP or VRRP configure static MAC entries for the Virtual MAC addresses.

Chapter 26 - Troubleshooting

This handbook chapter describes concepts of troubleshooting and solving issues that may occur with FortiGate units.

This FortiOS Handbook chapter contains the following chapters:

Verifying FortiGate admin access security explains how to verify and configure administrative access.

Troubleshooting resources walks you through Fortinet's resources for troubleshooting.

Troubleshooting tools describes some of the basic commands and parts of FortiOS that can help you with troubleshooting.

Troubleshooting methodologies walks you through best practice concepts of FortiOS troubleshooting.

Technical Support Organization Overview describes how Fortinet Support operates, what they will need from you if you contact them, and what you can expect in general.

Common questions answers most of the common questions.

Troubleshooting methodologies

Before you begin troubleshooting anything but the most minor issues, you need to prepare. Doing so will shorten the time to solve your issue. This section helps to explain how you prepare before troubleshooting, as well as creating a troubleshooting plan and contacting support.

This section contains the following topics:

- Establish a baseline
- Define the problem
- Gathering Facts
- Create a troubleshooting plan
- Obtain any required additional equipment
- Ensure you have administrator level access to required equipment
- Contact Fortinet customer support for assistance

Establish a baseline

FortiGate units operate at all layers of the OSI model. For this reason troubleshooting problems can become complex. If you establish a normal operation parameters, or baseline, for your system before the problem occurs it will help reduce the complexity when you are troubleshooting.

Many of the guiding questions in the following sections are some form of comparing the current problem situation to normal operation on your FortiGate unit. For this reason it is a best practice that you know what your normal operating status is, and have a record of it you can refer to. This can easily be accomplished by monitoring the system performance with logs, SNMP tools, or regularly running information gathering commands and saving the output. This regular operation data will show trends, and enable you to see when changes happen and there may be a problem.

Back up your FortiOS configuration on a regular basis. This is a good practice for every-day as well as when troubleshooting. You can restore the backed up configuration when needed and save the time and effort of re-creating it from the factory default settings.

Some fundamental CLI commands you can use to obtain normal operating data for your system:

`get system status`	Displays versions of firmware and FortiGuard engines, and other system information.
`get system performance status`	Displays CPU and memory states, average network usage, average sessions and session setup rate, virus caught, IPS attacks blocked, and uptime.
`get hardware memory`	Displays informations about memory
`get system session status`	Displays total number of sessions
`get router info routing-table all`	Displays all the routes in the routing table including their type, source, and other useful data.
`get ips session`	Displays memory used and max available to IPS as well and counts.
`get webfilter ftgd-statistics`	Displays list of FortiGuard related counts of status, errors, and other data.
`diagnose firewall statistic show`	Displays the amount of network traffic broken down into categories such as email, VoIP, TCP, UDP, IM, Gaming, P2P, and Streaming.
`diag system session list`	Displays current detailed sessions list
`show system dns`	Displays configured DNS servers
`diag sys ntp status`	Displays informations about ntp servers

These commands are just a sample. Feel free to include any extra information gathering commands that apply to your system. For example if you have active VPN connections, record information about them using the `get vpn *` series of commands.

For an extensive snapshot of your system, run the CLI command used by TAC to gather extensive information about a system — `exec tac report`. It runs many diagnostic commands that are for specific configurations. This means no matter what features you are using, this command will record their current state. Then if you need to perform troubleshooting at a later date, you can run the same command again and compare the differences to quickly locate suspicious output you can investigate.

Define the problem

The following questions can help determine the scope of the problem and isolate it:

- **What is the problem?**
  Do not assume that the problem is being experienced is the actual problem. First determine that the problem does not lie elsewhere before starting to troubleshoot the FortiGate device.

- **Has it ever worked before?**
  If the device never worked from the first day, you may not want to spend time troubleshooting something that could

well be defective. See “Troubleshooting bootup”.

- **Can the problem be reproduced at will or is it intermittent?**
  If the problem is intermittent, it may be dependent on system load. Also an intermittent problem can be very difficult to troubleshoot due to the difficulty reproducing the issue.

- **What has changed**?
  Do not assume that nothing has changed in the network. Use the FortiGate event log to see if any configuration changes were made. The change could be in the operating environment, for example, a gradual increase in load as more sites are forwarded through the firewall.

  If something has changed, see what the affect is if the change is rolled back.

- **Determine the scope of the problem - after you have isolated the problem what applications, users, devices, and operating systems does it effect?**

Before you can solve a problem, you need to understand it. Often this step can be the longest in this process.

Ask questions such as:

- What is not working? Be specific.
- Is there more than one thing not working?
- Is it partly working? If so, what parts are working?
- Is it a connectivity issue for the whole device, or is there an application that isn’t reaching the Internet?

Be as specific as possible with your answers, even if it takes awhile to find the answers.

These questions will help you define the problem. Once the problem is defined, you can search for a solution and then create a plan on how to solve it.

Gathering Facts

Fact gathering is an important part of defining the problem. Record the following information as it applies to the problem:

- Where did the problem occur?
- When did the problem occur and to whom?
- What components are involved?
- What is the affected application?
- Can the problem be traced using a packet sniffer?
- Can the problem be traced in the session table or using system debugging?
- Can log files be obtained that indicate a failure has occurred?

Answers to these questions will help you narrow down the problem, and what you have to check during your troubleshooting. The more things you can eliminate, the fewer things you need to check during troubleshooting. For this reason, be as specific and accurate as you can while gathering facts.

Create a troubleshooting plan

Once you have defined the problem, and searched for a solution you can create a plan to solve that problem. Even if your search didn't find a solution to your problem you may have found some additional things to check to further define your problem.

The plan should list all the possible causes of the problem that you can think of, and how to test for each possible cause.

Your troubleshooting plan will act as a checklist so that you know what you have tried and what is left to check. This is important to have if more than one person will be doing the troubleshooting. Without a written plan, people will become easily confused and steps will be skipped. Also if you have to hand over the problem to someone else, providing them with a detailed list of what data has been gathered and what solutions have been already tried demonstrates a good level of professionalism.

Be ready to add to your plan as needed. After you are part way through, you may discover that you forgot some tests or a test you performed discovered new information. This is normal.

Also if you contact support, they will require information about your problem as well as what you have already tried to fix the problem. This should all be part of your plan.

Providing Supporting Elements

If the Fortinet Technology Assistance Center (TAC) needs to be contacted to help you with your issue, be prepared to provide the following information:

- The firmware build version (use the `get system status` command)
- A network topology diagram
- A recent configuration file
- Optionally, a recent debug log
- Tell the support team what troubleshooting steps have already been performed and the results.

Do not provide the output from exec tac report unless Support requests it. The output from that command is very large and is not required in many cases.

For additional information about contacting Fortinet Customer Support, see Technical Support Organization Overview.

All of this is your troubleshooting plan.

Obtain any required additional equipment

You may require additional networking equipment, computers, or other equipment to test your solution.

Normally network administrators have additional networking equipment available either to loan you, or a lab where you can bring the FortiGate unit to test.

If you do not have access to equipment, check for shareware applications that can perform the same task. Often there are software solutions when hardware is too expensive.

Ensure you have administrator level access to required equipment

Before troubleshooting your FortiGate unit, you will need administrator access to the equipment. If you are a client on a FortiGate unit with virtual domains enabled, often you can troubleshoot within your own VDOM. However, you should inform your FortiGate unit's super admin that you will be doing troubleshooting.

Also, you may need access to other networking equipment such as switches, routers, and servers to help you test. If you do not normally have access to this equipment, contact your network administrator for assistance.

Contact Fortinet customer support for assistance

You have defined your problem, researched a solution, put together a plan to find the solution, and executed that plan. At this point if the problem has not been solved, its time to contact Fortinet Customer Support for assistance.

For more information, see Technical Support Organization Overview.

Troubleshooting tools

FortiOS provides a number of tools that help with troubleshooting both hardware and software issues. These tools include diagnostics and ports; ports are used when you need to understand the traffic coming in or going out on a specific port, for example, UDP 53, which is used by the FortiGate unit for DNS lookup and RBL lookup.

This section also contains information about troubleshooting FortiGuard issues.

This section contains the following topics:

- FortiOS diagnostics
- FortiOS ports
- FortiAnalyzer/FortiManager ports
- FortiGuard troubleshooting

FortiOS diagnostics

A collection of diagnostic commands are available in FortiOS for troubleshooting and performance monitoring. Within the CLI commands, the two main groups of diagnostic commands are `get` and `diagnose` commands. Both commands display information about system resources, connections, and settings that enable you to locate and fix problems, or to monitor system performance.

This topic includes diagnostics commands to help with:

- Check date and time
- Resource usage
- Proxy operation
- Hardware NIC
- Traffic trace
- Session table
- Firewall session setup rate
- Finding object dependencies
- Flow trace
- Packet sniffing and packet capture
- NPU based interfaces
- Debug command
- The execute tac report command
- Other commands

Check date and time

The system date and time are important for FortiGuard services, when logging events, and when sending alerts. The wrong time will make the log entries confusing and difficult to use.

Use Network Time Protocol (NTP) to set the date and time if possible. This is an automatic method that does not require manual intervention. However, you must ensure the port is allowed through the firewalls on your network. FortiToken synchronization requires NTP in many situations.

How to check the date and time - web-based manager

1. Go to **System Information > System Time** on the dashboard.
   Alternately, you can check the date and time using the CLI commands `execute date` and `execute time`.
2. If required, select **Change** to adjust the date and time settings.
   You can set the time zone, date and time, and select NTP usage. In the CLI, use the following commands to change the date and time:

```
config system global
   set timezone (use ? to get a list of IDs and descriptions of their timezone)
   end
config system ntp
   set type custom
      config ntpserver
         edit 1
            set server "ntp1.fortinet.net"
         next
         edit 2
            set server "ntp2.fortinet.net"
         next
   end
set ntpsync enable
set syncinterval 60
end
```

Resource usage

Each program running on a computer has one or more processes associated with it. For example if you open a Telnet program, it will have an associated telnet process. The same is true in FortiOS. All the processes have to share the system resources in FortiOS including memory and CPU.

Use `get system performance status` command to show the FortiOS performance status.

Sample output:

```
FGT#get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
CPU0 states: 0% user 0% system 0% nice 100% idle
CPU1 states: 0% user 0% system 0% nice 100% idle
CPU2 states: 0% user 0% system 0% nice 100% idle
CPU3 states: 0% user 0% system 0% nice 100% idle
Memory states: 25% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 5 sessions in 10 minutes, 4 sessions in 30
    minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second
    in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 12 hours, 7 minutes
```

Monitor the CPU/memory usage of internal processes using the following command:

```
get system performance top <delay> <max_lines>
```

The data listed by the command includes the name of the daemon, the process ID, whether the process is sleeping or running, the CPU percentage being used, and the memory percentage being used.

Sample output:

```
FGT#get system performance top 10 100
Run Time: 0 days, 11 hours and 30 minutes
0U, 0S, 100I; 1977T, 1470F, 121KF

    pyfcgid       120       S              0.0            1.3
    pyfcgid       121       S              0.0            1.3
    pyfcgid       122       S              0.0            1.3
    pyfcgid        53       S              0.0            1.3
  ipsengine        75       S <            0.0            1.3
  ipsengine        66       S <            0.0            1.3
  ipsengine        73       S <            0.0            1.3
  ipsengine        74       S <            0.0            1.3
  ipsengine        79       S <            0.0            1.3
  ipsengine        80       S <            0.0            1.3
    cmdbsvr        43       S              0.0            1.0
proxyworker       110       S              0.0            1.0
proxyworker       111       S              0.0            1.0
     httpsd       125       S              0.0            0.8
     httpsd        52       S              0.0            0.8
     httpsd       124       S              0.0            0.8
     newcli       141       R              0.0            0.7
     newcli       128       S              0.0            0.7
      fgfmd       102       S              0.0            0.7
       iked        86       S              0.0            0.7
```

Proxy operation

Monitor proxy operations using the following command:

```
diag test application <application> <option>
```

The `<application>` value can include the following:

`http`	HTTP proxy.
`smtp`	SMTP proxy.
`ftpd`	FTP proxy.
`pop3`	POP3 proxy.
`imap`	IMAP proxy.
`nntp`	NNTP proxy.
`proxyacceptor`	Proxy acceptor.
`proxyworker`	Proxy worker.
`scanunit`	Scanning unit.
`sslacceptor`	SSL proxy.
`sslworker`	SSL proxy.
`ssh`	SSH proxy.
`harelay`	HA relay daemon.
`hasync`	HA sync daemon.
`forticldd`	FortiCloud daemon.
`miglogd`	Miglog logging daemon.
`urlfilter`	URL filter daemon.
`ovrd`	Override daemon.
`ipsmonitor`	ips monitor
`ipsengine`	ips sensor
`ipldbd`	IP load balancing daemon.
`ddnscd`	DDNS client daemon.
`snmpd`	SNMP daemon.
`acd`	Aggregate Controller.
`dnsproxy`	DNS proxy.

sflowd	sFlow daemon.
init	init process.
l2tpcd	L2TP client daemon.
dhcprelay	DHCP relay daemon.
pptpcd	PPTP client.
wccpd	WCCP daemon.
wad	WAD related processes.
radiusd	RADIUS daemon.
sqldb	SQL database daemon.
reportd	Report daemon.
dlpfingerprint	DLP fingerprint daemon.
dlpfpcache	DLP fingerprint cache daemon.
wpad	WPA daemon.
fsd	FortiExplorer daemon.
ipsufd	IPS urlfilter daemon.
stp	Spanning Tree Protocol daemon.
lted	USB LTE daemon.
swctrl_authd	Switch controller authentication daemon.
forticron	Forticron daemon.
uploadd	Upload daemon.
quarantined	Quarantine daemon.
dhcp6c	DHCP6 client daemon.
info-sslvpnd	SSL-VPN info daemon.
thmd	Traffic history monitor daemon.
dsd	DLP Statistics daemon.

lnkmtd	Link monitor daemon.
dhcp6r	DHCP6 relay daemon.
fnbamd	Fortigate non-blocking auth daemon.

The <option> value depends from the application value used in the command. Here are some examples:

- If the application is http, the CLI command will be:

```
diag test application http <option>
```

The <option> value can be one from the following:

2	Drop all connections.
22	Drop max idle connections.
222	Drop all idle connections.
4	Display connection stat.
44	Display info per connection.
444	Display connections per state.
4444	Display per-VDOM statistics.
44444	Display information about idle connections.
55	Display tcp info per connection.
6	Display ICAP information.
70	Disable ICAP 'Allow: 204' (default).
71	Enable ICAP 'Allow: 204' .
72	Drop all ICAP server connections.
11	Display the SSL session ID cache statistics.
12	Clear the SSL session ID cache statistics.
13	Display the SSL session ID cache.
14	Clear the SSL session ID cache.
80	Show Fortinet bar SSL-VPN bookmark info.
81	Show Fortinet bar SSL-VPN bookmark cache.
82	Show Fortinet bar SSL-VPN bookmark LRU list.

- If the application is `ipsmonitor`, the CLI command will be

```
diag test application ipsmonitor <option>
```

The `<option>` value can be one from the following:

1	Display IPS engine information
2	Toggle IPS engine enable/disable status
3	Display restart log
4	Clear restart log
5	Toggle bypass status
6	Submit attack characteristics now
10	IPS queue length
11	Clear IPS queue length
12	IPS L7 socket statistics
13	IPS session list
14	IPS NTurbo statistics
15	IPSA statistics
97	Start all IPS engines
98	Stop all IPS engines
99	Restart all IPS engines and monitor

Hardware NIC

Monitor hardware network operations using the following command:

```
diag hardware deviceinfo nic <interface>
```

The information displayed by this command is important as errors at the interface are indicative of data link or physical layer issues which may impact the performance of the FortiGate unit.

The following is sample output when `<interface>` = `internal`:

```
System_Device_Name port5
Current_HWaddr 00:09:0f:68:35:60
Permanent_HWaddr 00:09:0f:68:35:60
Link up
Speed 100
Duplex full
[……]
Rx_Packets=5685708
Tx_Packets=4107073
Rx_Bytes=617908014
Tx_Bytes=1269751248
Rx_Errors=0
Tx_Errors=0
```

```
Rx_Dropped=0
Tx_Dropped=0
[…..]
```

The `diag hardware deviceinfo nic` command displays a list of hardware related error names and values. The following table explains the items in the list and their meanings.

Possible hardware errors and meanings

Field	Definition
Rx_Errors = rx error count	Bad frame was marked as error by PHY.
Rx_CRC_Errors + Rx_Length_Errors - Rx_Align_Errors	This error is only valid in 10/100M mode.
Rx_Dropped or Rx_No_Buffer_Count	Running out of buffer space.
Rx_Missed_Errors	Equals Rx_FIFO_Errors + CEXTERR (Carrier Extension Error Count). Only valid in 1000M mode, whichis marked by PHY.
Tx_Errors = Tx_Aborted_ Errors	ECOL (Excessive Collisions Count). Only valid in half-duplex mode.
Tx_Window_Errors	LATECOL (Late Collisions Count). Late collisions are collisions that occur after 64-byte time into the transmission of the packet while working in 10 to100Mb/s data rate and 512-byte timeinto the transmission of the packet while working in the 1000Mb/s data rate. This register only increments if transmits are enabled and the device is in half-duplex mode.
Rx_Dropped	See Rx_Errors.
Tx_Dropped	Not defined.
Collisions	Total number of collisions experienced by the transmitter. Valid in half-duplex mode.
Rx_Length_Errors	Transmission length error.
Rx_Over_Errors	Not defined.
Rx_CRC_Errors	Frame CRC error.
Rx_Frame_Errors	Same as Rx_Align_Errors. This error is only valid in 10/100M mode.
Rx_FIFO_Errors	Same as Rx_Missed_Errors - a missed packet count.
Tx_Aborted_Errors	See Tx_Errors.
Tx_Carrier_Errors	The PHY should assert the internal carrier sense signal during every transmission. Failure to do so may indicate that the link has failed or the PHY has an incorrect link configuration. This register only increments if transmits are enabled. This register is not valid in internal SerDes 1 mode (TBI mode for the 82544GC/EI) and is only valid when the Ethernet controller is operating at full duplex.
Tx_FIFO_Errors	Not defined.

Field	Definition
Tx_Heartbeat_Errors	Not defined.
Tx_Window_Errors	See LATECOL.
Tx_Single_Collision_Frames	Counts the number of times that a successfully transmitted packed encountered a single collision. The value only increments if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Multiple_Collision_Frames	A Multiple Collision Count which counts the number of times that a transmit encountered more than one collision but less than 16. The value only increments if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Deferred	Counts defer events. A defer event occurs when the transmitter cannot immediately send a packet due to the medium being busy because another device is transmitting, the IPG timer has not expired, half-duplex deferral events are occurring, XOFF frames are being received, or the link is not up. This register only increments if transmits are enabled. This counter does not increment for streaming transmits that are deferred due to TX IPG.
Rx_Frame_Too_Longs	The Rx frame is over size.
Rx_Frame_Too_Shorts	The Rx frame is too short.
Rx_Align_Errors	This error is only valid in 10/100M mode.
Symbol Error Count	Counts the number of symbol errors between reads - SYMERRS. The count increases for every bad symbol received, whether or not a packet is currently being received and whether or not the link is up. This register only increments in internal SerDes mode.

Traffic trace

Traffic tracing allows a specific packet stream to be followed. This is useful to confirm packets are taking the route you expected on your network.

View the characteristics of a traffic session though specific security policies using:

```
diag sys session
```

Trace per-packet operations for flow tracing using:

```
diag debug flow
```

Trace per-Ethernet frame using:

```
diag sniffer packet
```

Session table

A session is a communication channel between two devices or applications across the network. Sessions enable FortiOS to inspect and act on a sequential group of packets in a session all together instead of inspecting each

packet individually. Each of these sessions has an entry in the session table that includes important information about the session.

Use as a tool

Session tables are useful troubleshooting tools because they allow you to verify connections that you expect to see open. For example, if you have a web browser open to browse the Fortinet website, you would expect a session entry from your computer, on port 80, to the IP for the Fortinet website. Another troubleshooting method is if there are too many sessions for FortiOS to process, you can examine the session table for evidence why this is happening.

The FortiGate session table can be viewed from either the CLI or the web-based manager. The most useful troubleshooting data comes from the CLI. The session table in web-based manager also provides some useful summary information, particularly the current policy number that the session is using.

Web-based manager session information

In the web-based manager you can view session information in the FortiView page. Sessions are categorized by **Sources, Applications, Destinations,** and **All Sessions**.

How to find which security policy a specific connection is using

Every program and device on your network must have a communication channel, or session, open to pass information. The FortiGate unit manages these sessions with its many features from traffic shaping, to antivirus scanning, and even blocking known bad web sites. Each session has an entry in the session table.

You may want to find information for a specific session, say a secure web browser session, for troubleshooting. For example if that web browser session is not working properly, you can check the session table to ensure the session is still active, and that it is going to the proper address. It can also tell you the security policy number it matches, so you can check what is happening in that policy.

1. **Know your connection information.**
   You need to be able to identify the session you want. For this you need the source IP address (usually your computer), the destination IP address if you have it, and the port number which is determined by the program being used. Some commons ports are:
   - port 80 (HTTP for web browsing),
   - port 22 (SSH used for secure login and file transfers)
   - port 23 (telnet for a text connection)
   - port 443 (HTTPS for secure web browsing

2. **Find your session and policy ID.**
   Follow **System > FortiView> All Sessions**. Find your session by finding your source IP address, destination IP address if you have it, and port number. The policy ID is listed after the destination information. If the list of sessions is very long, you can filter the list to make it easier to find your session.

3. **When there are many sessions, use a filter to help you find your session.**
   If there are multiple pages of sessions it is difficult to find a single session. To help you in your search you can use a filter to block out sessions that you don't want. Click the search icon on the column heading to select the filter. Select **Source IP** and enter your source IP address. Now only sessions

that originate from your IP address will be displayed in the session table. If the list is still too long, you can do the same for the **Source port**. That will make it easy to find your session and the security policy ID. When you are finished remember to clear the filters.

CLI session information

The session table output from the CLI (`diag sys session list`) is very verbose. Even on a system with a small amount of traffic, displaying the session table will generate a large amount of output. For this reason, filters are used to display only the session data of interest.

You can filter a column in the web-based manager by clicking the search icon on the column heading or from the CLI by creating a filter.

An entry is placed in the session table for each traffic session passing through a security policy. The following command will list the information for a session in the table:

```
diag sys session list
```

Sample Output:

```
FGT# diag sys session list
session info: proto=6 proto_state=05 expire=89 timeout=3600 flags=00000000 av_idx=0 use=3
bandwidth=204800/sec guaranteed_bandwidth=102400/sec traffic=332/sec prio=0
    logtype=session ha_id=0 hakey=4450
tunnel=/
state=log shape may_dirty
statistic(bytes/packets/err): org=3408/38/0 reply=3888/31/0 tuples=2
orgin->sink: org pre->post, reply pre->post oif=3/5 gwy=192.168.11.254/10.0.5.100
hook=post dir=org act=snat 10.0.5.100:1251->192.168.11.254:22(192.168.11.105:1251)
hook=pre dir=reply act=dnat 192.168.11.254:22->192.168.11.105:1251(10.0.5.100:1251)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 domain_info=0 auth_info=0 ftgd_info=0 ids=0x0 vd=0 serial=00007c33 tos=ff/ff
```

Since output can be verbose, the filter option allows specific information to be displayed, for example:

```
diag sys session filter <option>
```

The `<option>` values available include the following:

clear	Clear session filter.
dintf	Destination interface.
dport	Destination port.
dst	Destination IP address.
duration	duration
expire	expire
negate	Inverse filter.
nport	NAT'd source port
nsrc	NAT'd source ip address
policy	Policy ID.
proto	Protocol number.
proto-state	Protocol state.
sintf	Source interface.
sport	Source port.
src	Source IP address.
vd	Index of virtual domain. -1 matches all.

Even though UDP is a sessionless protocol, the FortiGate unit still keeps track of the following two different states:

- UDP reply not seen with a value of 0
- UDP reply seen with a value of 1

The following illustrates FW session states from the session table:

State	Meaning
log	Session is being logged.
local	Session is originated from or destined for local stack.
ext	Session is created by a firewall session helper.
may_dirty	Session is created by a policy. For example, the session for `ftp control channel` will have this state but `ftp data channel` will not. This is also seen when NAT is enabled.
ndr	Session will be checked by IPS signature.
nds	Session will be checked by IPS anomaly.
br	Session is being bridged (TP) mode.

Firewall session setup rate

The number of sessions that can be established in a set period of time is useful information. A session is an end-to-end TCP/IP connection for communication with a limited lifespan. If you record the setup rate during normal operation, when you experience problems you have that setup rate with the current number to see if its very different. While this will not solve your problems, it can be a useful step to help you define your problem.

A reduced firewall session setup rate could be the result of a number of things from a lack of system resources on the FortiGate unit, to reaching the limit of your session count for your VDOM.

To view your session setup rate method 1- CLI

```
FGT# get sys performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 10% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes,
13 kbps in 30 minutes
Average sessions: 31 sessions in 1 minute, 30 sessions in 10
minutes, 31 sessions in 30 minutes
Average session setup rate: 0.5 sessions per second in last 1
minute, 0 sessions per second in last 10 minutes, 0 sessions per
second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 44 days, 18 hours, 42 minutes
```

The information you are looking for is the Average sessions section, highlighted in the above output. In this example you can see there were 31 sessions in 1 minute, or an average of 0.5 sessions per second. The values for 10 minutes and 30 minutes allow you to take a longer average for a more reliable value if your FortiGate unit is working at maximum capacity. The smallest FortiGate unit can have 1 000 sessions established per second across the unit.

Remember that session setup rate is a global command. If you have multiple VDOMs configured with many sessions in each one, the session setup rate per VDOM will be slower than if there were no VDOMs configured.

Finding object dependencies

An administrator may not be permitted to delete a configuration object if there are other configuration objects that depend on it. This command identifies other objects which depend on or *make reference to* the configuration object in question. If an error is displayed that an object is in use and cannot be deleted, this command can help identify the source of the problem.

Another use is if you have a virtual interface with objects that depend on it, you need to find and remove those dependencies before you delete that interface.

CLI method

When running multiple VDOMs, this command is run in the Global configuration only and it searches for the named object both in the Global and VDOM configuration most recently used:

```
diag sys checkused <path.object.mkey>
```

For example, to verify which objects are referred to in a security policy with an ID of 1, enter the command as follows:

```
diag sys checkused firewall.policy.policyid 1
```

To check what is referred to by interface `port1`, enter the following command:

```
diag sys checkused system.interface.name port1
```

To show all the dependencies for an interface, enter the command as follows:

```
diag sys checkused system.interface.name <interface name>
```

Sample Output:

```
entry used by table firewall.address:name '10.98.23.23_host'
entry used by table firewall.address:name 'NAS'
entry used by table firewall.address:name 'all'
entry used by table firewall.address:name 'fortinet.com'
entry used by table firewall.vip:name 'TORRENT_10.0.0.70:6883'
entry used by table firewall.policy:policyid '21'
entry used by table firewall.policy:policyid '14'
entry used by table firewall.policy:policyid '19'
```

In this example, the interface has dependent objects, including four address objects, one VIP, and three security policies.

Web-based manager method

In the web-based manager, the object dependencies for an interface can be easily checked and removed.

To remove interface object dependencies - web-based manager

1. Go to **System > Interfaces**.
   The number in the **Ref.** column is the number of objects that refer to this interface.
2. Select the number in the **Ref.** column for the desired interface.
   A Window listing the dependencies will appear.

3. Use these detailed entries to locate and remove object references to this interface.
   The trash can icon will change from gray when all object dependencies have been removed.
4. Remove the interface by selecting the check box for the interface, and select **Delete**.

Flow trace

To trace the flow of packets through the FortiGate unit, use the following command:

```
diag debug flow trace start
```

If your network is using IPv4, follow packet flow by setting a flow filter using this command:

```
diag debug flow filter <option>
```

Filtering options include the following:

`addr` IPv4 address
`clear` clear filter
`daddr` destination IPv4 address
`dport` destination port
`negate` inverse IPv4 filter
`port` port
`proto` protocol number
`saddr` source IPv4 address
`sport` source port
`vd` index of virtual domain, -1 matches all

If your network is using IPv6, follow packet flow by setting a flow filter using this command:

```
diag debug flow filter6 <option>
```

Filtering options include the following:

`addr` IPv6 address
`clear` clear filter
`daddr` destination IPv6 address
`dport` destination port
`negate` inverse IPv6 filter
`port` port
`proto` protocol number
`saddr` source IPv6 address
`sport` source port
`vd` index of virtual domain, -1 matches all

Enable the output to be displayed to the CLI console using the following command:

```
diag debug flow show console enable
```

`diag debug flow` output is recorded as event log messages and are sent to a FortiCloud or a FortiAnalyzer unit if connected. Do not let this command run longer than necessary since it generates significant amounts of data.

Start flow monitoring with a specific number of packets using this command:

```
diag debug flow trace start <N>
```

Stop flow tracing at any time using:

```
diag debug flow trace stop
```

The following is an example of the flow trace for the device at the following IP address: `203.160.224.97`

```
diag debug enable
diag debug flow filter addr 203.160.224.97
diag debug flow show console enable
diag debug flow show function-name enable
diag debug flow trace start 100
```

Flow trace output example - HTTP

Connect to the web site at the following address to observe the debug flow trace. The display may vary slightly:

```
http://www.fortinet.com
```

Comment: SYN packet received:

```
id=20085 trace_id=209 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

SYN sent and a new session is allocated:

```
id=20085 trace_id=209 func=resolve_ip_tuple line=2799
msg="allocate a new session-00000e90"
```

Lookup for next-hop gateway address:

```
id=20085 trace_id=209 func=vf_ip4_route_input line=1543
msg="find a route: gw-192.168.11.254 via port6"
```

Source NAT, lookup next available port:

```
id=20085 trace_id=209 func=get_new_addr line=1219
msg="find SNAT: IP-192.168.11.59, port-31925"
direction"
```

Matched security policy. Check to see which policy this session matches:

```
id=20085 trace_id=209 func=fw_forward_handler line=317
msg="Allowed by Policy-3: SNAT"
```

Apply source NAT:

```
id=20085 trace_id=209 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

SYN ACK received:

```
id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2700
msg="vd-root received a packet(proto=6, 203.160.224.97:80-
>192.168.11.59:31925) from port6."
```

Found existing session ID. Identified as the reply direction:

```
id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2727
msg="Find an existing session, id-00000e90, reply direction"
```

Apply destination NAT to inverse source NAT action:

```
id=20085 trace_id=210 func=__ip_session_run_tuple
line=1516 msg="DNAT 192.168.11.59:31925-
>192.168.3.221:1487"
```

Lookup for next-hop gateway address for reply traffic:

```
id=20085 trace_id=210 func=vf_ip4_route_input line=1543
msg="find a route: gw-192.168.3.221 via port5"
```

ACK received:

```
id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2700
msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

Match existing session in the original direction:

```
id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2727
msg="Find an existing session, id-00000e90, original
direction"
```

Apply source NAT:

```
id=20085 trace_id=211 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

Receive data from client:

```
id=20085 trace_id=212 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

Match existing session in the original direction:

```
id=20085 trace_id=212 func=resolve_ip_tuple_fast
line=2727 msg="Find an existing session, id-00000e90,
original direction"
```

Apply source NAT:

```
id=20085 trace_id=212 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

Receive data from server:

```
id=20085 trace_id=213 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
203.160.224.97:80->192.168.11.59:31925) from port6."
```

Match existing session in reply direction:

```
id=20085 trace_id=213 func=resolve_ip_tuple_fast
line=2727 msg="Find an existing session, id-00000e90,
reply direction"
```

Apply destination NAT to inverse source NAT action:

```
id=20085 trace_id=213 func=__ip_session_run_tuple
```

```
line=1516 msg="DNAT 192.168.11.59:31925-
>192.168.3.221:1487"
```

Flow trace output example - IPsec (policy-based)

```
id=20085 trace_id=1 msg="vd-root received a packet(proto=1, 10.72.55.240:1->10.71.55.10:8)
    from internal."
id=20085 trace_id=1 msg="allocate a new session-00001cd3"
id=20085 trace_id=1 msg="find a route: gw-66.236.56.230 via wan1"
id=20085 trace_id=1 msg="Allowed by Policy-2: encrypt"
id=20085 trace_id=1 msg="enter IPsec tunnel-RemotePhase1"
id=20085 trace_id=1 msg="encrypted, and send to 15.215.225.22 with source 66.236.56.226"
id=20085 trace_id=1 msg="send to 66.236.56.230 via intf-wan1"
id=20085 trace_id=2 msg="vd-root received a packet (proto=1, 10.72.55.240:1-1071.55.10:8)
    from internal."
id=20085 trace_id=2 msg="Find an existing session, id-00001cd3, original direction"
id=20085 trace_id=2 msg="enter IPsec ="encrypted, and send to 15.215.225.22 with source
    66.236.56.226" tunnel-RemotePhase1"
id=20085 trace_id=2 msgid=20085 trace_id=2 msg="send to 66.236.56.230 via intf-wan1"
```

Packet sniffing and packet capture

FortiOS devices can sniff packets using commands in the CLI or capture packets using the web-based manager. The differences between the two methods are not large.

Packet sniffing in the CLI is well suited for spot checking traffic from the CLI, but if you have complex filters to enter it can be a lot of work to enter them each time. You can also save the sniffing output; however, you must log to a file and then analyze the file later by hand.

Packet capture in the web-based manager makes it easy to set up multiple filters at once and just run one or two as you need them. You also have controls to start and stop capturing as you wish. Packet capture output is downloaded to your local computer as a *.pcap file which requires a third party application to read the file, such as Wireshark. This method is useful to send Fortinet support information to help resolve an issue.

Features	Packet sniffing	Packet capture
Command location	CLI	web-based manager
Third party software required	puTTY to log plaintext output	Wireshark to read *.pcap files
Read output in plain text file	yes	no
Read output as *.pcap file using Wireshark	no	yes
Easily configure single quick and simple filter	yes	no
Record packet interface	yes	no
Configure complex sniffer filters on multiple interface	no	yes
sniff IPv6	hard	easy
sniff non-IP packets	no	yes
Filter packets by protocol and/or port	easy	easy
Filter packets by source and/or destination address	easy	easy

Packet sniffing

Before you start sniffing packets on the CLI, you should be prepared to capture the output to a file — there can be huge amounts of data that you will not be able to see without saving it to a file. One method is to use a terminal program like puTTY to connect to the FortiGate unit's CLI. Then once the packet sniffing count is reached you can end the session and analyze the output in the file.

Details within packets passing through particular interfaces can be displayed using the packet sniffer with the following command:

```
diag sniffer packet <interface> <filter> <verbose> <count> <tsformat>
```

The `<interface>` value is required, with the rest being optional. If not included the default values will be `"none"`.

For example the simplest valid sniffer command would be:

```
diag sniffer packet any
```

The `<interface>` value can be any physical or virtual interface name. Use *any* to sniff packets on all interfaces.

The `<filter>` value limits the display of packets using filters, including Berkeley Packet Filtering (BPF) syntax. The `<filter>` value must be enclosed in quotes.

```
'[[src|dst] host <host_name_or_IP1>] [[src|dst] host <host_name_or_IP2>]
    [[arp|ip|ip6|gre|esp|udp|tcp] [port_no]] [[arp|ip|ip6|gre|esp|udp|tcp] [port_no]]'
```

If a second host is specified in the filter, only the traffic between the two hosts will be displayed. Optionally, you can use logical OR to match only one of the hosts, or match one of multiple protocols or ports. When defining a port, there are up to two parts — protocol and port number.

For example, to display UDP 1812 traffic or TCP 8080 traffic, use the following:

```
'udp port 1812 or tcp port 8080'
```

To display all IP traffic that has a source of 192.168.1.2 and a destination of 192.168.2.3:

```
'ip src host 192.168.1.2 and dst host 192.168.2.3'
```

The <verbose> option allows different levels of information to be displayed. The verbose levels include:

1 Print header of packets

2 Print header and data from the IP header of the packets

3 Print header and data from the Ethernet header of the packets

4 Print header of packets with interface name

5 Print header and data from ip of packets with interface name

6 Print header and data from ethernet of packets with interface name

The <count> value indicates the number of packets to sniff before stopping. If this variable is not included, or is set to zero, the sniffer will run until you manually halt it with Ctrl-C.

The <tsformat> value define the format of timestamp. It can be:

a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms

l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms

otherwise: relative to the start of sniffing, ss.ms

Packet capture

FortiOS 5.2 includes packet capture to the web-based manager. The FortiGate unit must have a disk and then capture-packet feature can be enabled from the CLI within the firewall policy as below:

```
config firewall policy
   edit <id>
   set capture-packet enable
end
```

To configure packet capture filters, go to **System > Network > Packet Capture**.

When you add a packet capture filter, enter the following information and select **OK**.

Interface	Select the interface to sniff from the dropdown menu. You must select one interface. You cannot change the interface without deleting the filter and creating a new one, unlike the other fields.
Max Packets to Capture	Enter the number of packets to capture before the filter stops. This number cannot be zero. You can halt the capturing before this number is reached.
Enable Filters	Select this option to specify your filter fields
Host(s)	Enter one or more hosts IP address Separate multiple hosts with commas. Enter a range using a dash without spaces, for example 172.16.1.5-172.16.1.15 or enter a subnet.
Port(s)	Enter one or more ports to capture on the selected interface. Separate multiple ports with commas. Enter a range using a dash without spaces, for example 88-90
VLAN(s)	Enter one or more vlans (if there is any). Separate multiple vlans with commas.
Protocol	Enter one or more protocol. Separate multiple protocol with commas. Enter a range using a dash without spaces, for example 1-6, 17, 21-25
Include IPv6 packets	Select this option if you are troubleshooting IPv6 networking, or if your network uses IPv6. Otherwise, leave it disabled.
Capture Non-IP packets	The protocols available in the list are all IP based except for ICMP (ping). To capture non-IP based packets select this feature. Some examples of non-IP packets include IPsec, IGMP, ARP, and as mentioned ICMP.

If you select a filter and go back to edit it, you have the added option of starting and stopping packet capture in the edit window, or downloading the captured packets. You can also see the filter status and the number of packets captured.

You can also select the filter and select **Start** to start capturing packets. While the filter is running, you will see the number of captured packets increasing until it reaches the max packet count or you select **Stop**. While the filter is running you cannot download the output file.

When the packet capture is complete, you can select **Download** to send the packet capture filter captured packets to your local computer as a *.pcap file. To read this file format, you will need to use Wireshark or a similar third party application. Using this tool you will have extensive analytics available to you and the full contents of the packets that were captured.

NPU based interfaces

Many Fortinet products contain network processors such as NP1, NP2, and NP4 network processors. Therefore offloading requirements, vary by network processor model.

When using the NPU-based interfaces, only the initial session setup will be seen through the `diag debug flow` command. If the session is correctly programmed into the ASIC (fastpath), the debug flow command will no longer see the packets arriving at the CPU. If the NPU functionality is disabled, the CPU will see all the packets, however, this should only be used for troubleshooting purposes.

First, obtain the NP4 id and the port numbers with the following command:

```
diag npu np4 list
```

Sample output:

```
ID Model Slot Interface
0 On-board port1 fabric1 fabric3 fabric5
1 On-board fabric2 port2 base2 fabric4
```

Run the following commands:

```
diag npu np4 fastpaf th disable <dev_id>
```

(where `dev_id` is the NP4 number)

Then, run this command:

```
diag npu np4 fastpath-sniffer enable port1
```

Sample output:

```
NP4 Fast Path Sniffer on port1 enabled
```

This will cause all traffic on **port1** of NP4 to be sent to the CPU meaning a standard sniffer trace can be taken and other diag commands should work if it was a standard CPU driven port.

These commands are only for the newer NP4 interfaces.

Debug command

Debug output provides continuous, real-time event information. Debugging output continues until it is explicitly stopped or until the unit is rebooted. Debugging output can affect system performance and will be continually generated even though output might not be displayed in the CLI console.

Debug information displayed in the console will scroll in the console display and may prevent CLI commands from being entered, for example, the command to disable the debug display. To turn off debugging output as the display is scrolling by, press the ↑ key to recall the recent diag debug command, press backspace, and type “0”, followed by **Enter**.

Debug output display is enabled using the following command:

```
diag debug enable
```

When finished examining the debug output, disable it using:

```
diag debug disable
```

Once enabled, indicate the debug information that is required using this command:

```
diag debug <option> <level>
```

Debug command options include the following:

`enable`	Enable debug output.
`disable`	Disable debug output.
`info`	Show active debug level settings.
`reset`	Reset all debug level to default.
`report`	Report for tech support.
`crashlog`	Crash log info.
`config-error-log`	Configure error log info.
`sql-log-error`	SQL log database error info.
`application`	application.
`kernel`	kernel.
`remote-extender`	remote-extender.
`console`	console.
`cli`	Debug CLI.
`cmdb-trace`	Trace CLI.
`rating`	Display rating info.
`authd`	Authentication daemon.
`fsso-polling`	FSSO active directory poll module.
`flow`	Trace packet flow in kernel.
`urlfilter`	urlfilter.
`admin`	Admin user.

The debug level can be set at the end of the command. Typical values are 2 and 3, for example:

```
diag debug application DHCPS 2
diag debug application spamfilter 2
```

Fortinet support will advise which debugging level to use.

Timestamps can be enabled to the debug output using the following command:

```
diag debug console timestamp enable
```

Debug output example

This example shows the IKE negotiation for a secure logging connection from a FortiGate unit to a FortiAnalyzer system.

```
diag debug reset
diag vpn ike log-filter src-addr4 192.168.11.2
diag debug enable
```

Sample Output:

```
FGh_FtiLog1: IPsec SA connect 0 192.168.11.2->192.168.10.201:500, natt_mode=0 rekey=0
    phase2=FGh_FtiLog1
FGh_FtiLog1: using existing connection, dpd_fail=0
FGh_FtiLog1: found phase2 FGh_FtiLog1
FGh_FtiLog1: IPsec SA connect 0 192.168.11.2 -> 192.168.10.201:500 negotiating
FGh_FtiLog1: overriding selector 225.30.5.8 with 192.168.11.2
FGh_FtiLog1: initiator quick-mode set pfs=1536...
FGh_FtiLog1: try to negotiate with 1800 life seconds.
FGh_FtiLog1: initiate an SA with selectors: 192.168.11.2/0.0.0.0->192.168.10.201,
    ports=0/0, protocol=0/0
Send IKE Packet(quick_outI1):192.168.11.2:500(if0) -> 192.168.10.201:500, len=348
Initiator: sent 192.168.10.201 quick mode message #1 (OK)
FGh_FtiLog1: set retransmit: st=168, timeout=6.
```

In this example:

`192.168.11.2->192.168.10.201:500`	Source and Destination gateway IP address
`dpd_fail=0`	Found existing Phase 1
`pfs=1536...`	Create new Phase 2 tunnel

The execute tac report command

`exec tac report` is an execute command that runs an exhaustive series of diagnostic commands. It runs commands that are only needed if you are using certain features like HA, VPN tunnels, or a modem. The report takes a few minutes to complete due to the amount of output generated. If you have your CLI output logged to a file, you can run this command to familiarize yourself with the CLI commands involved.

When you call Fortinet Customer Support, you will be asked to provide information about your unit and its current state using the output from this CLI command.

Other commands

ARP table

To view the ARP cache, use the following command:

```
get sys arp
```

To view the ARP cache in the system, use this command:

```
diag ip arp list
```

Sample output:

```
index=14 ifname=internal 224.0.0.5 01:00:5e:00:00:05 state=00000040 use=72203
    confirm=78203 update=72203 ref=1
index=13 ifname=dmz 192.168.3.100 state=00000020 use=1843 confirm=650179 update=644179
    ref=2 ? VIP
index=13 ifname=dmz 192.168.3.109 02:09:0f:78:69:ff state=00000004 use=71743 confirm=75743
    update=75743 ref=1
index=14 ifname=internal 192.168.11.56 00:1c:23:10:f8:20 state=00000004 use=10532
    confirm=10532 update=12658 ref=4
```

To remove the ARP cache, use this command:

```
execute clear system arp table
```

To remove a single ARP entry, use:

```
diag ip arp delete <interface name> <IP address>
```

To add static ARP entries, use the following command:

```
config system arp-table
```

Time and date settings

Check time and date settings for log message timestamp synchronization (the Fortinet support group may request this) and for certificates that have a time requirement to check for validity. Use the following commands:

```
execute time
current time is: 12:40:48
last ntp sync:Thu Mar 16 12:00:21 2006
execute date
current date is: 2006-03-16
```

To force synchronization with an NTP server, toggle the following command:

```
Config system ntp
   set ntpsync enable/disable
end
```

If all devices have the same time, it helps to correlate log entries from different devices.

IP address

There may be times when you want to verify the IP addresses assigned to the FortiGate unit interfaces are what you expect them to be. This is easily accomplished from the CLI using the following command.

```
diag ip address list
```

The output from this command lists the IP address and mask if available, the index of the interface (a sort of ID number) and the devname is the name of the interface. While physical interface names are set, virtual interface names can vary. Listing all the virtual interface names is a good use of this command. For vsys_ha and vsys_ fgfm, the IP addresses are the local host — these are internally used virtual interfaces.

```
# diag ip address list
IP=10.31.101.100->10.31.101.100/255.255.255.0 index=3 devname=internal
IP=172.20.120.122->172.20.120.122/255.255.255.0 index=5 devname=wan1
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=8 devname=root
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=11 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=13 devname=vsys_fgfm
```

FortiOS ports

In the TCP and UDP stacks, there are 65 535 ports available for applications to use when communicating with each other. Many of these ports are commonly known to be associated with specific applications or protocols. These known ports can be useful when troubleshooting your network.

Use the following ports while troubleshooting the FortiGate device:

Port(s)	Functionality
UDP 53	DNS lookup, RBL lookup
UDP 53 or UDP 8888	FortiGuard Antispam or Web Filtering rating lookup
UDP 53 (default) or UDP 8888 and UDP 1027 or UDP 1031	FDN Server List - source and destination port numbers vary by originating or reply traffic. See the article “How do I troubleshoot performance issues when FortiGuard Web Filtering is enabled?” in the Knowledge Base.
UDP 123	NTP Synchronization
UDP 162	SNMP Traps
UDP 514	SYSLOG - All FortiOS versions can use syslog to send log messages to remote syslog servers. FortiOS v2.80 and v3.0 can also view logs stored remotely on a FortiAnalyzer unit.
TCP 22	Configuration backup to FortiManager unit or FortiGuard Analysis and Management Service.
TCP 25	SMTP alert email, encrypted virus sample auto-submit
TCP 389 or TCP 636	LDAP or PKI authentication
TCP 443	FortiGuard Antivirus or IPS update - When requesting updates from a FortiManager unit instead of directly from the FDN, this port must be reconfigured as TCP 8890.
TCP 443	FortiGuard Analysis and Management Service
TCP 514	FortiGuard Analysis and Management Service log transmission (OFTP)
TCP 541	SSL Management Tunnel to FortiGuard Analysis and Management Service (FortiOS v3.0 MR6 or later)
TCP 514	Quarantine, remote access to logs and reports on a FortiAnalyzer unit, device registration with FortiAnalyzer units (OFTP)
TCP 1812	RADIUS authentication
TCP 8000 and TCP 8002	FSSO
TCP 10151	FortiGuard Analysis and Management Service contract validation

FortiAnalyzer/FortiManager ports

If you have a FortiAnalyzer unit or FortiManager unit on your network you may need to use the following ports for troubleshooting network traffic.

Functionality	Port(s)
DNS lookup	UDP 53
NTP synchronization	UDP 123
Windows share	UDP 137-138
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514
Log and report upload	TCP 21 or TCP 22
SMTP alert email	TCP 25
User name LDAP queries for reports	TCP 389 or TCP 636
RVS update	TCP 443
RADIUS authentication	TCP 1812
Log aggregation client	TCP 3000

FortiGuard troubleshooting

The FortiGuard service provides updates to Antivirus, Antispam, IPS, Webfiltering, and more. The FortiGuard Distribution System (FDS) involves a number of servers across the world that provide updates to your FortiGate unit. Problems can occur both with connection to FDS, and its configuration on your local FortiGate unit. Some of the more common troubleshooting methods are listed here including

- Troubleshooting process for FortiGuard updates
- FortiGuard server settings

Troubleshooting process for FortiGuard updates

The following process are the logical steps to take when troubleshooting FortiGuard update problems. This includes antivirus (AV), intrusion protection services (IPS), antispam (AS), and web filtering (WB).

1. **Does the device have a valid licence that includes these services?**
   Each device requires a valid FortiGuard license to access updates for some or all of these services. You can verify the support contract status for your devices at the Fortinet Support website — https://support.fortinet.com/.
2. **If the device is part of an HA cluster, do all members of the cluster have the same level of support?**
   As with the previous step, you can verify the support contract status for all the devices in your HA cluster at the Fortinet Support website.
3. **Have services been enabled on the device?**
   To see the FortiGuard information and status for a device, in the web-based manager go to **System > Config > FortiGuard**. On that page you can verify the status of each component, and if required enable each service. If there are problems, see the FortiGuard section of the FortiOS Handbook.

4. **Is the device able to communicate with FortiGuard servers?**
   At **System > Config > FortiGuard** you can also attempt to update AV and IPS, or test the availability of WF and AS default and alternate ports. If there are problems, see the FortiGuard section of the FortiOS Handbook.
5. **Is there proper routing to reach the FortiGuard servers?**
   Ensure there is a static or dynamic route that enables your ForitGate unit to reach the FortiGuard servers. Usually a generic default route to the internet is enough, but you may need to verify this if your network is complex.
6. **Are there issues with DNS?**
   An easy way to test this is to attempt a traceroute from behind the FortiGate unit to an external network using the FQDN for a location. If the traceroute FQDN name does not resolve, you have general DNS problems.
7. **Is there anything upstream that might be blocking FortiGuard traffic, either on the network or ISP side?**
   Many firewalls block all ports by default, and often ISPs block ports that are low. There may be a firewall between the FortiGate unit and the FortiGuard servers that is blocking the traffic. FortiGuard uses port 53 by default, so if it is being blocked you need to either open a hole for it, or change the port it is using.
8. **Is there an issue with source ports?**
   It is possible that ports used to contact FortiGuard are being changed before reaching FortiGuard or on the return trip before reaching your FortiGate unit. A possible solution for this is to use a fixed-port at NATd firewalls to ensure the port remains the same. Packet sniffing can be used to find more information on what is happening with ports.
9. **Are there security policies that include antivirus?**
   If no security policies include antivirus, the antivirus databse will not be updated. If antivirus is included, only the database type used will be updated.

FortiGuard server settings

Your local FortiGate unit connects to remote FortiGuard servers get updates to FortiGuard information such as new viruses that may have been found or other new threats. This section demonstrates ways to display information about FortiGuard server information on your FortiGate unit, and how to use that information and update it to fix potential problems.

Displaying the server list

The `get webfilter status` or `diag debug rating` command shows the list of FDS servers the FortiGate unit is using to send web filtering requests. Rating requests are only sent to the server on the top of the list in normal operation. Each server is probed for Round Trip Time (RTT) every two minutes.

You can optionally add a refresh rate to the end of this command and that will determine how often the server list will be refreshed.

Rating may not be enabled on your FortiGate unit.

```
get webfilter status
```

Sample Output:

```
Locale : english
License : Contract
Expiration : Thu Oct 9 02:00:00 2011
-=- Server List (Mon Feb 18 12:55:48 2008) -=-
```

IP	Weight	RTT	Flags	TZ	Packets	CurrLost	TotalLost
a.b.c.d	0	1	DI	2	1926879	0	11176

10.1.101.1	10	329	1	10263	0	633
10.2.102.2	20	169	0	16105	0	80
10.3.103.3	20	182	0	6741	0	776
10.4.104.4	20	184	0	5249	0	987
10.5.105.5	25	181	0	12072	0	178

Output Details

The Server List includes the IP addresses of alternate servers if the first entry cannot be reached. In this example the IP addresses are not public addresses

The following flags in `get webfilter status` indicate the server status:

- `D` - the server was found through the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with D and will be used first for INIT requests before falling back to the other servers.
- `I` - the server to which the last INIT request was sent.
- `F` - the server has not responded to requests and is considered to have failed.
- `T` - the server is currently being timed.
- `S` - means that rating requests can be sent to the server. The flag is set for a server only in two cases:
  1. The server exists in the servers list received from the Fortimanager or any other INIT server.
  2. The servers list received from the FortiManager is empty so the Fortimanager itself would be the only server known by Fortigate thus it should be used as the rating server.

  The servers that are not currently serving will be pushed down to the bottom list (under the available serving servers, and on top of the failed servers) in order for the `load-balance-servers` feature in the `config system fortiguard` to work properly.

Sorting the server list

The server list is sorted first by weight. The server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost (there has been no response in 2 seconds), it will be resent to the next server in the list. Therefore, the top position in the list is selected based on RTT while the other list positions are based on weight.

Calculating weight

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a remote server, the weight is not allowed to dip below a base weight, calculated as the difference in hours between the FortiGate unit and the server times 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Common questions

The general troubleshooting tips include, and can help answer, the following questions:

How to check hardware connections

- Are all the cables and interfaces connected properly?
- Is the LED for the interface green?

How to check FortiOS network settings

- If you are having problems connecting to the management interface, is your protocol enabled on the interface for administrative access?
- Is there an IP address on the interface?

How to check CPU and memory resources

- Is your CPU running at almost 100 percent usage?
- Are you running low on memory?

How to check modem status

- Is the modem connected?
- Are there PPP issues?

How to run ping and traceroute

- Are you experiencing complete packet loss?

How to check the logs

- Do you need to identify a problem?

How to verify the contents of the routing table (in NAT mode)

- Are there routes in the routing table for default and static routes?
- Do all connected subnets have a route in the routing table?
- Does a route wrongly have a higher priority than it should?

How to verify the correct route is being used

- Has the traffic been routed correctly?

How to verify the correct firewall policy is being used

- Is the correct firewall policy applied to the expected traffic?

How to check the bridging information in Transparent mode

- Are you having problems in Transparent mode?

How to check number of sessions used by UTM proxy

- Have you reached the maximum number of sessions for a protocol?
- Are new sessions failing to start for a certain protocol?

How to examine the firewall session list

- Are there active firewall sessions?

How to check wireless information

- Is the wireless network functioning properly?

How to verify FortiGuard connectivity

- Is the FortiGate unit communicating properly with FortiGuard?

How to perform a sniffer trace (CLI and Packet Capture)

- Is traffic entering the FortiGate unit and does it arrive on the expected interface?
- Is the ARP resolution correct for the next-hop destination?
- Is the traffic exiting the FortiGate unit to the destination as expected?
- Is the traffic being sent back to the originator?

How to debug the packet flow

- Is the traffic entering or leaving the FortiGate unit as expected?

How to check hardware connections

If there is no traffic flowing from the FortiGate unit, it may be a hardware problem.

To check hardware connections:

- Ensure the network cables are properly plugged into the interfaces.
- Ensure there are connection lights for the network cables on the unit.
- Change the cable if the cable or its connector are damaged or you are unsure about the cable's type or quality—such as straight through or crossover, or possibly exposed wires at the connector.
- Connect the FortiGate unit to different hardware.
- Ensure the link status is set to **Up** for the interface, (see **Network > Interface > Status)**. The link status is based on the physical connection and cannot be set in FortiOS.

If any of these solve the problem, it was a hardware connection problem. You should still perform some basic software connectivity tests to ensure complete connectivity. It might also be that the interface is disabled, or has its **Administrative Status** set to **Down**.

To enable an interface - web-based manager

1. Using the web-based management interface, go to **System > Network > Interface**.
2. Select and edit the interface to enable, such as **port1**.
3. Find **Administrative Status** at the bottom of the screen, and select **Up**.
4. Select **Apply**.

To enable an interface - CLI

```
config system interface
   edit port1
      set status up
   next
end
```

How to check FortiOS network settings

FortiOS network settings are present in both the web-based manager interface and the CLI. The following information includes troubleshooting and best practice information. The network settings include:

Interface settings

DNS settings

DHCP Server settings

Interface settings

If you can access the FortiGate unit with the management cable only, the first step is to display the interface settings. To display the settings for the internal interface, use the following CLI command:

```
FGT# show system interface <Interface_mane>
```

For a complete listing of all the possible interface settings, use the following CLI command:

```
config system interface
   edit <Interface_name>
   get
end
```

Check the interface settings to ensure they are not preventing traffic. Specific things to check include (only the web-based manager names are shown, CLI names may vary slightly):

- **Link Status —** *Down* until a valid cable is plugged into this interface, after which it will be **Up**. The Link Status is shown physically by the connection LED for the interface. If it lights up green, it is a good connection. If Link Status is *Down*, the interface does not work. Link Status is also displayed on the **System > Network > Interface** screen by default.
- **Addressing mode —** Do not use **DHCP** if you don't have a DHCP server —you will not be able to logon to an interface in DHCP mode as it will not have an IP address.
- **IP/Netmask —** An interface needs an IP address to be able to connect to other devices. Ensure there is a valid IP address in this field. The one exception is if **DHCP** is enabled for this interface to get its IP address from an external DHCP server.
- **IPv6 address —** The same protocol must be used by both ends to complete the connection. Ensure both this interface and the remote connection are both using IPv4 or both using IPv6 addressing.
- **Administrative access —** If no protocols are selected, you will have to use the local management cable to connect to the unit. If you are using IPv6, configure the IPv6 administrative access protocols.
- **Administrative status —** Set to **Up** or the interface will not work.

DNS settings

While this section is not complicated, many networking problems can be traced back to DNS problems. Things to check in this area include:

- Are there values for both primary and secondary entries?
- Is the local domain name correct?
- Are you using IPv6 addressing? If so, are the IPv6 DNS settings correct?
- Are you using Dynamic DNS (DDNS)? If so, is it using the correct server, credentials, and interface?
- Can you contact both DNS servers to verify the servers are operational?

- If an interface addressing mode is set to DHCP and is set to override the internal DNS, is that interface receiving a valid DNS entry from the DHCP server? Is it a reasonable address and can it be contacted to verify it's operational?
- Are there any DENY security policies that need to allow DNS?
- Can any internal device perform a successful traceroute to a location using the FQDN?

DHCP Server settings

DHCP Servers are common on internal and wireless networks. If the DHCP server is not configured properly it can cause problems. Things to check in this area include:

- Is the DHCP server entry set to **Relay**? If so, verify there is another DHCP server to which requests can be relayed. Otherwise, it should be set to **Server**.
- Is the DHCP server enabled?
- Does this DHCP server use a valid range of IP addresses? Are those addresses in use by other devices? If one or more devices are using IP addresses in this range, you can use the IP reservation feature to ensure the DHCP server does not use these addresses.
- Is there a gateway entry? Include a gateway entry to ensure clients of this server have a default route.
- Is the system DNS setting being used? The best practice is to avoid confusion by using the system DNS whenever possible. However, the option to specify up to three custom DNS servers is available, and all three entries should be used for redundancy.

There are some situations, such as a new wireless interface, or during the initial FortiGate unit configuration, where interfaces override the system DNS entries. When this happens, it often shows up as intermittent Internet connectivity. To fix the problem, go to **System > Network > DNS** and ensure to enable **Use FortiGuard Servers**.

How to check CPU and memory resources

System resources are shared and a number of processes run simultaneously on the FortiGate unit. If one of these processes consumes nearly all the resources.

A quick way to monitor CPU and memory usage is on the System Dashboard using the **System Resources** widgets. They have both a visual gauge displayed to show you the usage.

To check the system resources on your FortiGate unit, run the following CLI command:

```
FGT# get system performance status
```

This command provides a quick and easy snapshot of the FortiGate.

The first line of output shows the CPU usage by category. A FortiGate that is doing nothing will look like:

```
CPU states: 0% user 0% system 0% nice 100% idle
```

However, if your network is running slow you might see something like:

```
CPU states: 1% user 98% system 0% nice 1% idle
```

This line shows that all the CPU is used up by system processes. Normally this should not happen as it shows the FortiGate is overloaded for some reason. If you see this overloading, you should investigate farther as it's possible a process, such as scanunitid, is using all the resources to scan traffic, in which case you need to reduce

the amount of traffic being scanned by blocking unwanted protocols, configuring more security policies to limit scanning to certain protocols, or similar actions. It is also possible that a hacker has gained access to your network and is overloading it with malicious activity such as running a spam server or using zombie PCs to attack other networks on the Internet. You can get additional CPU related information with the CLI command `get system performance top`. This command shows you all the top processes running on the FortiGate unit (names on the left) and their CPU usage. If a process is using most of the CPU cycles, investigate it to determine if it's normal activity.

The second line of output from `get system performance status` shows the memory usage. Memory usage should not exceed 90 percent. If memory is too full, some processes will not be able to function properly. For example, if the system is running low on memory, antivirus scanning will go into failopen mode where it will start dropping connections or bypass the antivirus system.

The other lines of output, such as average network usage, average session setup rate, viruses caught, and IPS attacks blocked can also help you determine why system resource usage it high. For example, if network usage is high it will result in high traffic processing on the FortiGate, or if the session setup rate is very low or zero the proxy may be overloaded and not able to do its job.

How to troubleshoot high memory usage

As with any system, FortiOS has a finite set of hardware resources such as memory and all the running processes share that memory. Depending on their workload, each process will use more or less as needed, usually more in high traffic situations. If some processes use all the available memory, other processes will have no memory available and not be able to function.

When high memory usage happens, you may experience services that appear to freeze up and connections are lost or new connections are refused.

If you are seeing high memory usage in the **System Resources** widget, it could mean that the unit is dealing with high traffic volume, which may be causing the problem, or it could be when the unit is dealing with connection pool limits affecting a single proxy. If the unit is receiving large volumes of traffic on a specific proxy, it is possible that the unit will exceed the connection pool limit. If the number of free connections within a proxy connection pool reaches zero, problems may occur.

Use the following CLI command, which uses the antivirus failopen feature. Setting it to idledrop will drop connections based on the clients that have the most connections open. This helps to determine the behavior of the FortiGate antivirus system if it becomes overloaded in high traffic.

```
config system global
   set av-failopen idledrop
end
```

Use the following CLI command, which gives you information about current memory usage:

```
   diagnose hardware sysinfo memory
```

Sample output:

```
total: used: free: shared: buffers: cached: shm:
Mem: 2074185728 756936704 1317249024 0 20701184 194555904 161046528
Swap:       0       0       0
MemTotal:   2025572 kB
MemFree:    1286376 kB
MemShared:        0 kB
Buffers:      20216 kB
Cached:      189996 kB
SwapCached:       0 kB
Active:       56644 kB
Inactive:    153648 kB
HighTotal:        0 kB
HighFree:         0 kB
LowTotal:   2025572 kB
LowFree:    1286376 kB
SwapTotal:        0 kB
SwapFree:         0 kB
```

How to troubleshoot high CPU usage

FortiOS has many features. If many of them are used at the same time, it can quickly use up all the CPU resources. When this happens, you will experience connection related problems stemming from the FortiOS unit trying to manage its workload by refusing new connections, or even more aggressive methods.

Some examples of features that are CPU intensive are VPN high level encryption, having all traffic undergo all possible scanning, logging all traffic, and packets, and dashboard widgets that frequently update their data.

1. **Determine how high the CPU usage is currently.** There are two main ways to do this. The easiest is to go to **System > Dashboard > Status** and look at the **system resources** widget. This is a dial gauge that displays a percentage use for the CPU. If its at the red-line, you should take action. The other method is to use the Dashboard CLI widget to enter `diag sys top`.

   Sample output:

   ```
   Run Time: 11 days, 23 hours and 36 minutes
   0U, 0S, 98I; 1977T, 758F, 180KF
           newcli 286 R 0.1 0.8
           ipsengine 78 S < 0.0 3.1
           ipsengine 64 S < 0.0 3.0
           ipsengine 77 S < 0.0 3.0
           ipsengine 68 S < 0.0 2.9
           ipsengine 66 S < 0.0 2.9
           ipsengine 79 S < 0.0 2.9
           scanunitd 133 S < 0.0 1.8
           pyfcgid 267 S 0.0 1.8
           pyfcgid 269 S 0.0 1.7
           pyfcgid 268 S 0.0 1.6
           httpsd 139 S 0.0 1.6
           pyfcgid 266 S 0.0 1.5
           scanunitd 131 S < 0.0 1.4
           scanunitd 132 S < 0.0 1.4
           proxyworker 90 S 0.0 1.3
           cmdbsvr 43 S 0.0 1.1
           proxyworker 91 S 0.0 1.1
           miglogd 55 S 0.0 1.1
   ```

```
httpsd 135 S 0.0 1.0
```

Where the codes displayed on the second output line mean the following:

- `U` is % of user space applications using CPU. In the example, `0U` means 0% of the user space applications are using CPU.
- `S` is % of system processes (or kernel processes) using CPU. In the example, `0S` means 0% of the system processes are using the CPU.
- `I` is % of idle CPU. In the example, `98I` means the CPU is 98% idle.
- `T` is the total FortiOS system memory in Mb. In the example, `1977T` means there are 1977 Mb of system memory.
- `F` is free memory in Mb. In the example, `758F` means there is 758 Mb of free memory.
- `KF` is the total shared memory pages used. In the example, `180KF` means the system is using 180 shared memory pages.

Each additional line of the command output displays information for each of the processes running on the FortiGate unit. For example, the third line of the output is:

```
newcli 286 R 0.1 0.8
```

Where:

- `newcli` is the process name. Other process names can include `ipsengine`, `sshd`, `cmdbsrv`, `httpsd`, `scanunitd`, and `miglogd`.
- `286` is the process ID. The process ID can be any number.
- `R` is the current state of the process. The process state can be:

- `R` running
- `S` sleep
- `Z` zombie
- `D` disk sleep.
  - `0.1` is the amount of CPU that the process is using. CPU usage can range from 0.0 for a process that is sleeping to higher values for a process that is taking a lot of CPU time.
  - `0.8` is the amount of memory that the process is using. Memory usage can range from 0.1 to 5.5 and higher.

Enter the following single-key commands when `diagnose sys top` is running:

- Press `q` to quit and return to the normal CLI prompt.
- Press `p` to sort the processes by the amount of CPU that the processes are using.
- Press `m` to sort the processes by the amount of memory that the processes are using.

2. **Determine what features are using most of the CPU resources.**
   There is a command in the CLI to let you see the top few processes currently running that use the most CPU resources. The CLI command `get system performance top` outputs a table of information. You are interested in the second most right column, CPU usage by percentage. If the top few entries are using most of the CPU, note which processes they are and investigate those features to try and reduce their CPU load. Some examples of processes you will see include:
   - `ipsengine` — the IPS engine that scans traffic for intrusions
   - `scanunitd` — antivirus scanner
   - `httpsd` — secure HTTP
   - `iked` — internet key exchange (IKE) in use with IPsec VPN tunnels

- `newcli` — active whenever you are accessing the CLI
- `sshd` — there are active secure socket connections
- `cmdbsrv` — the command database server application

Go to the features that are at the top of the list and look for evidence of them overusing the CPU. Generally the monitor for a feature is a good place to start.

3. Check for unnecessary CPU “wasters”.
These are some best practises that will reduce your CPU usage, even if you are not experiencing high CPU usage. Note that if you require a feature this section tells you to turn off, ignore it.
   - Use hardware acceleration wherever possible to offload tasks from the CPU. Offloading tasks such as encryption frees up the CPU for other tasks.
   - Avoid the use of GUI widgets that require computing cycles, such as the Top Sessions widget. These widgets are constantly polling the system for their information, which uses CPU and other resources.
   - Schedule antivirus, IPS, and firmware updates during off peak hours. Usually these don’t consume CPU resources but they can disrupt normal operation.
   - Check the log levels and which events are being logged. This is the severity of the messages that are recorded. Consider going up one level to reduce the amount of logging. Also if there are events you do not need to monitor, remove them from the list.
   - Log to FortiCloud instead of memory or Disk. Logging to memory quickly uses up resources. Logging to local disk will impact overall performance and reduce the lifetime of the unit. Fortinet recommends logging to FortiCloud which doesn’t use much CPU.
   - If the disk is almost full, transfer the logs or data off the disk to free up space. When a disk is almost full it consumes a lot of resources to find the free space and organize the files.
   - If you have packet logging enabled, consider disabling it. When it’s enabled it records every packet that comes through that policy.
   - Halt all sniffers and traces.
   - Ensure you are not scanning traffic twice. If traffic enters the FortiGate unit on one interface, goes out another, and then comes back in again that traffic does not need to be rescanned. Doing so is a waste of resources. However, ensure that traffic truly is being scanned once.
   - Reduce the session timers to close unused sessions faster. To do this in the CLI enter the following commands and values. These values reduce the values from defaults. Note that `tcp-timewait` has 10 seconds added by the system by default.

     ```
     config system global
        set tcp-halfclose-timer 30
        set tcp-halfopen-timer 30
        set tcp-timewait-timer 0
        set udp-idle-timer 60
     end
     ```
   - Enable only features that you need under **System > Config > Features**.

4. **When CPU usage is under control, use SNMP to monitor CPU usage. Alternately, use logging to record CPU and memory usage every 5 minutes.**
Once things are back to normal, you should set up a warning system to alert you of future CPU overusage. A common method to do this is with SNMP. SNMP monitors many values on the FortiOS and allows you to set high water marks that will generate events. You run an application on your computer to watch for and record these events. Go to **System > Config > SNMP** to enable and configure an SNMP community. If this method is too complicated, you can use the **System Resources** widget to record CPU usage. However, this method will not alert you to problems - it will just record them as they happen.

How to check modem status

Sometimes the modem may not work properly, or the unit may not be detecting the modem. Use the following diagnostic commands to help you troubleshoot issues with the modem.

```
diagnose sys modem {cmd | com | detect | history | external-modem| query| reset}
```

You should always run the following diagnose command after inserting the USB modem into the unit:

```
diagnose sys modem detect
```

You can view the modem configuration by using the `get system modem` command. You can also view the modem's vendor identification as well as the custom product identification number from the information output from the `get system modem` command.

When there are connectivity issues, use the following to help you resolve them:

- `diag debug enable` – activates the debug on the console
- `diag debug application modemd` – dumps communication between the modem and the unit.
- `diag debug application ppp` – dumps the PPP negotiating messages.
- `execute modem dial` – displays modem debug output.

The modem diagnose output should not contain any error on the way to initializing. You should also verify the number that is used to dial with your ISP.

How to run ping and traceroute

Ping and traceroute are useful tools in network troubleshooting. Alone, either one can determine network connectivity between two points. However, ping can be used to generate simple network traffic to view with diagnose commands on the FortiGate unit. This combination can be very powerful when locating network problems.

In addition to their normal uses, ping and traceroute can tell you if your computer or network device has access to a domain name server (DNS). While both tools can use IP addresses alone, they can also use domain names for devices. This is an added troubleshooting feature that can be useful in determining why particular services, such as email or web browsing, may not be working properly.

If ping does not work, you likely have it disabled on at least one of the interface settings, and security policies for that interface.

Both ping and traceroute require particular ports to be open on firewalls, or else they cannot function. Since you typically use these tools to troubleshoot, you can allow them in the security policies and on interfaces only when you need them, and otherwise keep the ports disabled for added security.

Ping

The ping command sends a very small packet to the destination, and waits for a response. The response has a timer that may expire, indicating the destination is unreachable. The behavior of ping is very much like a sonar ping from a submarine, where the command gets its name.

Ping is part of Layer-3 on the OSI Networking Model. Ping sends Internet Control Message Protocol (ICMP) “echo request” packets to the destination, and listens for “echo response” packets in reply. However, many public networks block ICMP packets because ping can be used in a denial of service (DoS) attack (such as Ping of Death or a smurf attack), or by an attacker to find active locations on the network. By default, FortiGate units have ping enabled while broadcast-forward is disabled on the external interface.

What ping can tell you

Beyond the basic connectivity information, ping can tell you the amount of packet loss (if any), how long it takes the packet to make the round trip, and the variation in that time from packet to packet.

If there is some packet loss detected, you should investigate the following:

- Possible ECMP, split horizon, or network loops.
- Cabling to ensure no loose connections.
- Verify which security policy was used (use the packet count column on the **Policy & Objects > Policy** page).

If there is total packet loss, you should investigate the following:

- **Hardware —** ensure cabling is correct, and all equipment between the two locations is accounted for.
- **Addresses and routes —** ensure all IP addresses and routing information along the route is configured as expected.
- **Firewalls —** ensure all firewalls, including FortiGate unit security policies allow PING to pass through.

How to use ping

Ping syntax is the same for nearly every type of system on a network.

To ping from a FortiGate unit

1. Connect to the CLI either through telnet or through the CLI widget on the web-based manager dashboard.
2. Enter `exec ping 10.11.101.101` to send 5 ping packets to the destination IP address. There are no options for this command.

   Sample output:

```
Head_Office_620b # exec ping 10.11.101.101
PING 10.11.101.101 (10.11.101.101): 56 data bytes
64 bytes from 10.11.101.101: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 10.11.101.101: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.11.101.101 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

To ping from an MS Windows PC

1. Open a command window.
   - In Windows XP, select **Start > Run**, enter cmd, and select **OK**.
   - In Windows 7, select the Start icon, enter cmd in the search box, and select cmd.exe from the list.
2. Enter `ping 10.11.101.100` to ping the default internal interface of the FortiGate unit with four packets.

Other options include:

- `-t` to send packets until you press “Control-C”
- `-a` to resolve addresses to domain names where possible
- `-n X` to send X ping packets and stop

Sample output:

```
C:\>ping 10.11.101.101

Pinging 10.11.101.101 with 32 bytes of data:
Reply from 10.11.101.101: bytes=32 time=10ms TTL=255
Reply from 10.11.101.101: bytes=32 time<1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255

Ping statistics for 10.11.101.101:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

To ping from a Linux PC

1. Go to a shell prompt.
2. Enter “`ping 10.11.101.101`”.

Traceroute

Where ping will only tell you if it reached its destination and came back successfully, traceroute will show each step of its journey to its destination and how long each step takes. If ping finds an outage between two points, traceroute can be used to locate exactly where the problem is.

What is traceroute

Traceroute works by sending ICMP packets to test each hop along the route. It will send out three packets, and then increase the time to live (TTL) setting by one each time. This effectively allows the packets to go one hop farther along the route. This is the reason why most traceroute commands display their maximum hop count before they start tracing the route — that is the maximum number of steps it will take before declaring the destination unreachable. Also, the TTL setting may result in steps along the route timing out due to slow responses. There are many possible reasons for this to occur.

By default, traceroute uses UDP datagrams with destination ports numbered from 33434 to 33534. The traceroute utility usually has an option to specify use of ICMP echo request (type 8) instead, as used by the Windows tracert utility. If you have a firewall and if you want traceroute to work from both machines (Unix-like systems and Windows) you will need to allow both protocols inbound through your FortiGate security policies (UDP with ports from 33434 to 33534 and ICMP type 8).

You can also use the packet count column of the **Policy & Objects > Policy** page to track traceroute packets. This allows you to verify the connection, but also confirm which security policy the traceroute packets are using.

What traceroute can tell you

Ping and traceroute have similar functions—to verify connectivity between two points. The big difference is that traceroute shows you each step of the way, where ping does not. Also, ping and traceroute use different protocols

and ports, so one may succeed where the other fails.

You can verify your DNS connection using traceroute. If you enter an FQDN instead of an IP address for the traceroute, DNS will try to resolve that domain name. If the name does not get resolved, you know you have DNS issues.

How to use traceroute

The traceroute command varies slightly between operating systems. Note that in MS Windows the command name is shortened to "`tracert`". Also, your output will list different domain names and IP addresses along your route.

To use traceroute on an MS Windows PC

1. Open a command window.
   - In Windows XP, select **Start > Run**, enter cmd, and select **OK**.
   - In Windows 7, select the Start icon, enter cmd in the search box, and select cmd.exe from the list.
2. Enter "`tracert fortinet.com`" to trace the route from the PC to the Fortinet web site.
   Sample output:

```
C:\>tracert fortinet.com

Tracing route to fortinet.com [208.70.202.225]
over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms 172.20.120.2
2 66 ms 24 ms 31 ms 209-87-254-xxx.storm.ca [209.87.254.221]
3 52 ms 22 ms 18 ms core-2-g0-0-1104.storm.ca [209.87.239.129]
4 43 ms 36 ms 27 ms core-3-g0-0-1185.storm.ca [209.87.239.222]
5 46 ms 21 ms 16 ms te3-x.1156.mpd01.cogentco.com [38.104.158.69]
6 25 ms 45 ms 53 ms te8-7.mpd01.cogentco.com [154.54.27.249]
7 89 ms 70 ms 36 ms te3-x.mpd01.cogentco.com [154.54.6.206]
8 55 ms 77 ms 58 ms sl-st30-chi-.sprintlink.net [144.232.9.69]
9 53 ms 58 ms 46 ms sl-0-3-3-x.sprintlink.net [144.232.19.181]
10 82 ms 90 ms 75 ms sl-x-12-0-1.sprintlink.net [144.232.20.61]
11 122 ms 123 ms 132 ms sl-0-x-0-3.sprintlink.net [144.232.18.150]
12 129 ms 119 ms 139 ms 144.232.20.7
13 172 ms 164 ms 243 ms sl-321313-0.sprintlink.net [144.223.243.58]
14 99 ms 94 ms 93 ms 203.78.181.18
15 108 ms 102 ms 89 ms 203.78.176.2
16 98 ms 95 ms 97 ms 208.70.202.225

Trace complete.
```

The first, or the left column, is the hop count, which cannot go over 30 hops. When that number is reached, the traceroute ends.

The second, third, and fourth columns display how much time each of the three packets takes to reach this stage of the route. These values are in milliseconds and normally vary quite a bit. Typically a value of `<1ms` indicates a local connection.

The fifth, or the column farthest to the right, is the domain name of that device and its IP address or possibly just the IP address.

To perform a traceroute on a Linux PC

1. Go to a command line prompt.
2. Enter "`traceroute fortinet.com`".

The Linux traceroute output is very similar to the MS Windows tracert output.

To perform a traceroute from the FortiGate

1. Connect to the CLI either through telnet or through the CLI widget on the web-based manager dashboard.
2. Enter `exec traceroute www.fortinet.com` to trace the route to the destination IP address. There are no options for this command.

   Output appears as follows:

```
# execute traceroute www.fortinet.com
traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte packets
1 172.20.120.2 0.637 ms 0.653 ms 0.279 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 2.448 ms 2.519 ms 2.458 ms
3 209.87.239.129 <core-2-g0-2.storm.ca> 2.917 ms 2.828 ms 9.324 ms
4 209.87.239.199 <core-3-bdi1739.storm.ca> 13.248 ms 12.401 ms 13.009 ms
5 216.66.41.113 <v502.core1.tor1.he.net> 17.181 ms 12.422 ms 12.268 ms
6 184.105.80.9 <100ge1-2.core1.nyc4.he.net> 21.355 ms 21.518 ms 21.597 ms
7 198.32.118.41 <ny-paix-gni.twgate.net> 83.297 ms 84.416 ms 83.782 ms
8 203.160.228.217 <217-228-160-203.TWGATE-IP.twgate.net> 82.579 ms 82.187 ms 82.066 ms
9 203.160.228.229 <229-228-160-203.TWGATE-IP.twgate.net> 82.055 ms 82.455 ms 81.808 ms
10 203.78.181.2 82.262 ms 81.572 ms 82.015 ms
11 203.78.186.70 83.283 ms 83.243 ms 83.293 ms
12 66.171.127.177 84.030 ms 84.229 ms 83.550 ms
13 66.171.121.34 <www.fortinet.com> 84.023 ms 83.903 ms 84.032 ms
14 66.171.121.34 <www.fortinet.com> 83.874 ms 84.084 ms 83.810 ms
```

How to check the logs

This step in troubleshooting can be forgotten, but its an important one. Logging records the traffic passing through the FortiGate unit to your network and what action the FortiGate unit took during its scanning process of the traffic. This recorded information is called a log message.

When you configure FortiOS initially, log as much information as you can. If needed, logging of unused features can be turned off or scaled back if the logs generated are too large.

As with most troubleshooting steps, before you can determine if the logs indicate a problem, you need to know what logs result from normal operation. Without a baseline it is difficult to properly troubleshoot.

When troubleshooting with log files:

- Compare current logs to a recorded baseline of normal operation.
- If needed increase the level of logging (such as from Warning to Information) to obtain more information.

When increasing logging levels, ensure that alert email is configured and both disk usage and log quota are selected. This ensures you will be notified if the increased logging causes problems. You can also use Logging Monitor (located in **Log&Report > Monitor > Logging volume Monitor**) to determine the activities that generate the most log entries.

- check all logs to ensure important information is not overlooked
- filter or order log entries based on different fields (such as level, service, or IP address) to look for patterns that may indicate a specific problem (such as frequent blocked connections on a specific port for all IP addresses)

Logs will help identify and locate any problems, but they will not solve the problems. The job of logs is to speed up your problem solving and save you time and effort.

For more information on Logging and Log Reports, see the Logging and Reporting handbook chapter.

How to verify the contents of the routing table (in NAT mode)

When you have some connectivity, or possibly none at all a good place to look for information is the routing table.

The routing table is where all the currently used routes are stored for both static and dynamic protocols. If a route is in the routing table, it saves the time and resources of a lookup. If a route is not used for a while and a new route needs to be added, the oldest least used route is bumped if the routing table is full. This ensures the most recently used routes stay in the table. If your FortiGate unit is in Transparent mode, you are unable to perform this step.

If the FortiGate is running in NAT mode, verify that all desired routes are in the routing table: local subnets, default routes, specific static routes, and dynamic routing protocols.

To check the routing table in the web-based manager, use the Routing Monitor by going to **Router > Monitor > Routing Monitor**.

In the CLI, use the command `get router info routing-table all`. Sample output:

```
FGT# get router info routing-table all

Codes:
        K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

S* 0.0.0.0/0 [10/0] via 172.20.120.2, wan1
C 10.31.101.0/24 is directly connected, internal
C 172.20.120.0/24 is directly connected, wan1
```

How to verify the correct route is being used

If you have more than one default route and wants to make sure that traffic is flowing as expected via the right route, you can run a trace route from a machine in the local area network, this will indicate you the first hop that the traffic goes through.

Sample output:

```
C:\>tracert www.fortinet.com

Tracing route to www.fortinet.com [66.171.121.34]
over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.10.1.99
2 1 ms <1 ms <1 ms 172.20.120.2
3 3 ms 3 ms 3 ms static-209-87-254-221.storm.ca [209.87.254.221]
4 3 ms 3 ms 3 ms core-2-g0-2.storm.ca [209.87.239.129]
5 13 ms 13 ms 13 ms core-3-bdi1739.storm.ca [209.87.239.199]
6 12 ms 19 ms 11 ms v502.core1.tor1.he.net [216.66.41.113]
7 22 ms 22 ms 21 ms 100ge1-2.core1.nyc4.he.net [184.105.80.9]
8 84 ms 84 ms 84 ms ny-paix-gni.twgate.net [198.32.118.41]
9 82 ms 84 ms 82 ms 217-228-160-203.TWGATE-IP.twgate.net [203.160.22
8.217]
10 82 ms 81 ms 82 ms 229-228-160-203.TWGATE-IP.twgate.net [203.160.22
8.229]
11 82 ms 82 ms 82 ms 203.78.181.2
12 84 ms 83 ms 83 ms 203.78.186.70
13 84 ms * 85 ms 66.171.127.177
14 84 ms 84 ms 84 ms fortinet.com [66.171.121.34]
15 84 ms 84 ms 83 ms fortinet.com [66.171.121.34]

Trace complete.
```

In this scenario, the first hop contains the IP address `10.10.1.99`, which is the internal interface of the FortiGate. The second hop contains the IP address `172.20.120.2`, to which the wan1 interface of the FortiGate is connected, so we can conclude that the route via wan1 interface is being used for this traffic.

Also debug the packet flow in the CLI shows the route taken for each session.

Sample output:

```
id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a route: gw-172.20.120.2
    via wan1"
```

For more information on debuging the packet flow, see How to debug the packet flow.

How to verify the correct firewall policy is being used

If you have more than one firewall policy, use the count column to check which policy is being used, the count must show traffic increasing. To do so, go to **Policy & Objects > Policy** page.

Also debuging the packet flow in the CLI shows the policy id allowing the traffic.

Sample output:

```
id=13 trace_id=1 func=fw_forward_handler line=650 msg="Allowed by Policy-14: SNAT"
```

For more information on debuging the packet flow, see How to debug the packet flow.

How to check the bridging information in Transparent mode

When FortiOS is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit.

Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed, that is a likely cause. Check for the MAC address of the interface or device in question.

How to check the bridging information

To list the existing bridge instances on the FortiGate unit, use the following command:

```
diagnose netlink brctl list
```

Sample output:

```
#diagnose netlink brctl list
list bridge information
1. root.b fdb: size=256 used=6 num=7 depth=2 simple=no
Total 1 bridges
```

How to display forwarding domain information

Forwarding domains, or collision domains, are used in routing to limit where packets are forwarded on the network. Layer-2 broadcasts are limited to the same group. By default, all interfaces are in group 0. For example, if the FortiGate unit has 12 interfaces, only two may be in the same forwarding domain, which will limit packets that are broadcast to only those two interfaces. This reduces traffic on the rest of the network.

Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. It is important to know what interfaces are part of which forwarding domains as this determines which interfaces can communicate with each other.

To manually configure forwarding domains in Transparent mode, use the following FortiOS CLI command:

```
config system interface
   edit <interface_name>
   set forward-domain <integer>
end
```

To display the information for forward domains

Use the following command:

```
diagnose netlink brctl domain <name> <id>
```

where <name> is the name of the forwarding domain to display and <id> is the domain id.

Sample output

```
diagnose netlink brctl domain ione 101
show bridge root.b ione forward domain.
id=101 dev=trunk_1 6
```

To list the existing bridge MAC table, use the following command:

```
diagnose netlink brctl name host <name>
```

Sample output

```
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
```

port no	device	devname	mac addr	ttl	attributes
2	7	wan2	02:09:0f:78:69:00	0	Local Static
5	6	vlan_1	02:09:0f:78:69:01	0	Local Static
3	8	dmz	02:09:0f:78:69:01	0	Local Static
4	9	internal	02:09:0f:78:69:02	0	Local Static
3	8	dmz	00:80:c8:39:87:5a	194	
4	9	internal	02:09:0f:78:67:68	8	
1	3	wan1	00:09:0f:78:69:fe	0	Local Static

To list the existing bridge port list, use this command:

```
diagnose netlink brctl name port <name>
```

Sample Output:

```
show bridge root.b data port.
trunk_1 peer_dev=0
```

```
internal peer_dev=0
dmz peer_dev=0
wan2 peer_dev=0
wan1 peer_dev=0
```

How to check number of sessions used by UTM proxy

Each FortiGate model has a set limit of the maximum number of sessions the UTM proxy supports. The UTM proxy handles all the traffic for the following protocols: HTTP, SMTP, POP3, IMAP, FTP, and NNTP. If the proxy for a protocol fills up its session table, the FortiGate unit will enter conserve mode, where it behaves differently, until entries and memory free up again.

Conserve or failopen mode

Once you reach the limit, depending on your FortiGate unit's conserve mode configuration, no new sessions are created until an old ones end. You can configure your FortiGate unit's behavior when memory is running low or the proxy connection limit has been reached. There are two related commands for this in the CLI:

```
config system global
   set av-failopen-session {enable | disable}
   set av-failopen { idledrop | off | one-shot | pass}
end
```

`av-failopen-session` must be enabled to set the behavior for these conditions. When it is enabled, and a proxy for a protocol runs out of room in its session table that protocol goes into failopen mode and behaves as defined in the `av-failopen` command.

`av-failopen` determines the behavior of the proxy until entries are free in the session table again for that proxy.

- **idledrop —** This option removes idle sessions from the session table, starting with the clients that have the most sessions currently open. This method assumes that idle sessions are not being used and it will not cause problems to close these sessions. This is usually true, but some applications may have problems with this and start complaining about either not having or being able to open a session. If this occurs, try another method to check if this is really the problem. This is a secure option as no unscanned traffic is allowed to pass.
- **off —** This option turns off accepting any new AV sessions, but will continue to process any existing AV sessions that are currently active. All the protocols listed (HTTP, SMTP, POP3, IMAP, FTP, and NNTP) are scanned by FortiGate Antivirus. If AV scanning is enabled, av-failopen off is selected, and the proxy session table fills up, then no new sessions of that type will be accepted. For example, if POP3 session table is filled and email AV scanning is enabled, no more POP3 connections will be allowed until the session table gets some free space. This is a secure option because no unscanned traffic is allowed to pass.
- **one-shot —** When memory is low, bypass the antivirus system. The name one-shot comes from the fact that once you are in one-shot av-failopen mode, you must set av-failopen to either *pass* or *off* to restart AV scanning. This is a very unsecure option because it allows all traffic without AV scanning, and it never reverts to normal without manual assistance.
- **pass —** When memory is low, bypass the antivirus system much as one-shot. The difference is that when memory is freed up, the system will start AV scanning automatically again. This is an unsecure option because it allows traffic to pass without AV scanning. However, it is better than one-shot because it automatically restarts AV scanning when possible.

If the proxy session table is full for one or more protocols and your FortiGate unit enters into conserve or failopen mode, it will appear as if you have lost connections, network services are intermittent or non-existent, and yet other services work normally for a while until their sessions end and they join the queue of session-starved applications.

Checking sessions in use

To make troubleshooting this type of problem easier, sessions are broken down by which protocol they use. This provides you with statistics and errors specific to one of the protocols.

Due to the amount of output from this command, you should connect to the CLI with a terminal program, such as puTTY, that logs output. Otherwise, you will likely not be able to access all the output information from the command.

In the following output, only the HTTP entries are displayed. The other protocols have been removed in an attempt to shorten the output. There will be separate entries for each supported protocol (HTTP, SMTP, POP3, IMAP, FTP, and NNTP) in each section of the output.

To check sessions in use and related errors - CLI

```
FGT# # get test proxyworker 4

Worker[0]
HTTP Common
Current Connections 8/8032
Max Concurrent Connections 76


Worker Stat
Running time (HH:MM:SS:usec) 29:06:27:369365
Time in loop scanning 2:08:000198
Error Count (accept) 0
Error Count (read) 0
Error Count (write) 0
Error Count (poll) 0
Error Count (alloc) 0
Last Error 0
Acceptor Read 6386
Acceptor Write 19621
Acceptor Close 0

HTTP Stat
Bytes sent 667012 (kb)
Bytes received 680347 (kb)
Error Count (alloc) 0
Error Count (accept) 0
Error Count (bind) 0
Error Count (connect) 0
Error Count (socket) 0
Error Count (read) 134
Error Count (write) 0
Error Count (retry) 40
Error Count (poll) 0
Error Count (scan reset) 2
Error Count (urlfilter wait) 3
Last Error 104
Web responses clean 17950
Web responses scan errors 23
Web responses detected 16
Web responses infected with worms 0
```

```
Web responses infected with viruses 0
Web responses infected with susp 0
Web responses file blocked 0
Web responses file exempt 0
Web responses bannedword detected 0
Web requests oversize pass 16
Web requests oversize block 0
Last Server Scan errors 102
URL requests exempt 0
URL requests blocked 0
URL requests passed 0
URL requests submit error 0
URL requests rating error 0
URL requests rating block 0
URL requests rating allow 10025
URL requests infected with worms 0
Web requests detected 0
Web requests file blocked 0
Web requests file exempt 0
POST requests clean 512
POST requests scan errors 0
POST requests infected with viruses 0
POST requests infected with susp 0
POST requests file blocked 0
POST requests bannedword detected 0
POST requests oversize pass 0
POST requests oversize block 0
Web request backlog drop 0
Web response backlog drop 0


Worker Accounting
poll=721392/649809/42 pollfail=0 cmdb=85 scan=19266 acceptor=25975

HTTP Accounting
setup_ok=8316 setup_fail=0 conn_ok=0 conn_inp=8316
urlfilter=16553/21491/20 uf_lookupf=0
scan=23786 clt=278876 srv=368557

SMTP Accounting
setup_ok=12 setup_fail=0 conn_ok=0 conn_inp=12
scan=12 suspend=0 resume=0 reject=0 spamadd=0 spamdel=0 clt=275 srv=279

POP3 Accounting
setup_ok=30 setup_fail=0 conn_ok=0 conn_inp=30
scan=3 clt=5690 srv=5836

IMAP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
scan=0 clt=0 srv=0

FTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
scan=0 clt=0 srv=0 datalisten=0 dataclt=0 datasrv=0

NNTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
```

```
scan=0 clt=0 srv=0
```

The output from this command falls into the following sections:

- **HTTP Common current connections —** There is an entry for each protocol that displays the connections currently used, and the maximum connections allowed. This maximum is for the UTM proxy, which means all the protocols connections combined cannot be larger than this number. To support this, note that the maximum session count for each protocol is the same. You may also see a line titled `Max Concurrent Connections` for each protocol. This number is the maximum connections of this type allowed at one time. If VDOMs are enabled, this value is defined either on the global or per-VDOM level at **VDOM > Global Resources**.
- **Worker Stat —** This is statistics about the UTM proxy including how long it has been running, and how many errors it has found.
- **HTTP Stat —** This section includes statistics about the HTTP protocol proxy. This is a very extensive list covering errors, web responses, and any UTM positive matches. There are similar sections for each protocol, but the specific entries in each vary based on what UTM scanning is looking for in each — spam control for email, file transfer blocking for FTP, and so on.
- **Worker Accounting —** Lists accounting information about the UTM proxy such as polling statistics, how many sessions were scanned, and how many were just accepted. This information can tell you if expect AV scanning is taking place or not. Under normal operation there should be no errors or fails.
- **HTTP Accounting —** The accounting sections for each protocol provide information about successful session creation, failures, how many sessions are being scanned or filtered, and how many are client or server originated. If setup_fail is larger than zero, run the command again to see if it is increasing quickly. If it is, your FortiGate unit may be in conserve mode.

Related commands

To dump memory usage:

```
# get test proxyworker 1
```

To display statistics per VDOM:

```
# get test proxyworker 4444
```

To restart the proxy:

```
# get test proxyworker 99
```

How to examine the firewall session list

One further step is to examine the firewall session. The firewall session list displays all the sessions the FortiGate unit has open. You will be able to see if there are strange patterns such as no sessions apart from the internal network, or all sessions are only to one IP address.

When examining the firewall session list in the CLI, filters may be used to reduce the output. In the web-based manager, the filters are part of the interface.

To examine the firewall session list - web-based manager

- Go to **System > FortiView> All Sessions**.

To examine the firewall session list - CLI

When examining the firewall session list, there may be too many sessions to display. In this case it will be necessary to limit or filter the sessions displayed by source or destination address, or NATed address or port. If you want to filter by more than one of these, you need to enter a separate line for each value.

The following example shows filtering the session list based on a source address of 10.11.101.112.

```
FGT# diag sys session filter src 10.11.101.112
FGT# diag sys session list
```

The following example shows filtering the session list based on a destination address of 172.20.120.222.

```
FGT# diag sys session filter dst 172.20.120.222
FGT# diag sys session list
```

To clear all sessions corresponding to a filter - CLI

```
FGT# diag sys session filter dst 172.20.120.222
FGT# diag sys session clear
```

Check source NAT information

Remember NAT when troubleshooting connections. NAT is especially important if you are troubleshooting from the remote end of the connection outside the FortiGate unit firewall. On the dashboard session list, pay attention to **Src address after NAT**, and **Src port after NAT**. These columns display the IP and port values after NAT has been applied.

The NAT values can be helpful to ensure they are the values you expect, and to ensure the remote end of the sessions can see the expected IP address and port number.

When displaying the session list in the CLI, you can match the NATed source address (`nsrc`) and port (`nport`). This can be useful if multiple internal IP addresses are NATed to a common external facing source IP address.

```
FGT# diag sys session filter nsrc 172.20.120.122
FGT# diag sys session filter nport 8888
FGT# diag sys session list
```

How to check wireless information

Wireless connections, stations, and interfaces have different issues than other physical interfaces.

Troubleshooting station connection issue

To check whether station entry is created on Access Control:

```
FG600B3909600253 # diagnose wireless-controller wlac -d sta
* vf=0 wtp=70 rId=2 wlan=open ip=0.0.0.0 mac=00:09:0f:db:c4:03 rssi=0 idle=148 bw=0 use=2
vf=0 wtp=70 rId=2 wlan=open ip=172.30.32.122 mac=00:25:9c:e0:47:88 rssi=-40 idle=0 bw=9
    use=2
```

Enable diagnostic for particular station

This example uses the station MAC address to find where it is failing:

```
FG600B3909600253 # diagnose wireless-controller wlac sta_filter 00:25:9c:e0:47:88 1
Set filter sta 00:25:9c:e0:47:88 level 1
```

```
FG600B3909600253 # 71419.245 <ih> IEEE 802.11 mgmt::disassoc <== 00:25:9c:e0:47:88 vap
    open rId 1 wId 0 00:09:0f:db:c4:03
71419.246 <dc> STA del 00:25:9c:e0:47:88 vap open rId 1 wId 0
71419.246 <cc> STA_CFG_REQ(34) sta 00:25:9c:e0:47:88 del ==> ws (0-192.168.35.1:5246) rId
    1 wId 0
71419.246 <cc> STA del 00:25:9c:e0:47:88 vap open ws (0-192.168.35.1:5246) rId 1 wId 0
    00:09:0f:db:c4:03 sec open reason I2C_STA_DEL
71419.247 <cc> STA_CFG_RESP(34) 00:25:9c:e0:47:88 <== ws (0-192.168.35.1:5246) rc 0
    (Success).
```

How to verify FortiGuard connectivity

You can verify the FortiGuard connectivity in the **License Information** widget under **System > Dashboard > Status.** When FortiGate is connected to FortiGuard, a green check mark appears for available FortiGuard services.

From CLI, execute ping “service.fortiguard.net” and “update.fortiguard.net”.

Sample output:

```
FG100D# execute ping service.fortiguard.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=51 time=61.0 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=51 time=60.0 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=51 time=59.6 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=51 time=58.9 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=51 time=59.2 ms

--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 58.9/59.7/61.0 ms

FG100D# execute ping update.fortiguard.net
PING fds1.fortinet.com (208.91.112.68): 56 data bytes
64 bytes from 208.91.112.68: icmp_seq=0 ttl=53 time=62.0 ms
64 bytes from 208.91.112.68: icmp_seq=1 ttl=53 time=61.8 ms
64 bytes from 208.91.112.68: icmp_seq=2 ttl=53 time=61.3 ms
64 bytes from 208.91.112.68: icmp_seq=3 ttl=53 time=61.9 ms
64 bytes from 208.91.112.68: icmp_seq=4 ttl=53 time=61.8 ms
```

How to perform a sniffer trace (CLI and Packet Capture)

When troubleshooting networks and routing in particular, it helps to look inside the headers of packets to determine if they are traveling along the expected route. Packet sniffing can also be called a network tap, packet capture, or logic analyzing.

If your FortiGate unit has NP2/NP4 interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP2/NP4 interfaces, you should disable offloading on those interfaces.

What can sniffing packets tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, what the port of entry is on the FortiGate unit, if the ARP resolution is correct, and if the traffic is

being sent back to the source as expected.

Sniffing packets can also tell you if the FortiGate unit is silently dropping packets for reasons such as Reverse Path Forwarding (RPF), also called Anti Spoofing, which prevents an IP packet from being forwarded if its Source IP does not either belong to a locally attached subnet (local interface), or be part of the routing between the FortiGate unit and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymetric enable`), however this will disable stateful inspection on the FortiGate unit and cause many features to be turned off.

If you configure virtual IP addresses on your FortiGate unit, it will use those addresses in preference to the physical IP addresses. You will notice this when you are sniffing packets because all the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

How do you sniff packets

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

<interface_name>	The name of the interface to sniff, such as "port1" or "internal". This can also be "any" to sniff all interfaces.
<'filter'>	What to look for in the information the sniffer reads. "none" indicates no filtering, and all packets will be displayed as the other arguments indicate. The filter must be inside single quotes (‘).
<verbose>	The level of verbosity as one of: **1 -** print header of packets **2 -** print header and data from IP of packets **3 -** print header and data from Ethernet of packets **4 -** print header of packets with interface name
<count>	The number of packets the sniffer reads before stopping. If you do not put a number here, the sniffer will run forever unit you stop it with <CTRL C>.

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next three packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]

0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757
```

```
0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

For a more advanced example of packet sniffing, the following commands will report packets on any interface travelling between a computer with the host name of “PC1” and the computer with the host name of “PC2”. With verbosity 4 and above, the sniffer trace will display the interface names where traffic enters or leaves the FortiGate unit. Remember to stop the sniffer, type `CTRL+C`.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2>" 4
```

or

```
FGT# diagnose sniffer packet any "(host <PC1> or host <PC2>) and icmp" 4
```

The following sniffer CLI command includes the ARP protocol in the filter which may be useful to troubleshoot a failure in the ARP resolution (for instance PC2 may be down and not responding to the FortiGate ARP requests).

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4
```

Packet Capture

When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture can also be called a network tap, packet sniffing, or logic analyzing.

To use the packet capture:

1. Go to **System > Network > Packet Capture**.
2. Select the interface to monitor and select the number of packets to keep.
3. Select **Enable Filters**.
4. Enter the information you want to gather from the packet capture.
5. Select **OK**.

To run the capture, select the **play** button in the progress column in the packet capture list. If not active, **Not Running** will also appear in the column cell. The progress bar will indicate the status of the capture. You can stop and restart it at any time.

When the capture is complete, click the **Download** icon to save the packet capture file to your hard disk for further analysis.

Packet capture tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- Finding missing traffic.
- Seeing if sessions are setting up properly.
- Locating ARP problems such as broadcast storm sources and causes.
- Confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks.
- Confirming routing is working as you expect.
- Wireless client connection problems.
- Intermittent missing PING packets.
- A particular type of packet is having problems, such as UDP, which is commonly used for streaming video.

If you are running a constant traffic application such as ping, packet capture can tell you if the traffic is reaching the destination, how the port enters and exits the FortiGate unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start capturing packets, you need to have a good idea of what you are looking for. Capture is used to confirm or deny your ideas about what is happening on the network. If you try capture without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to capture enough packets to really understand all of the patterns and behavior that you are looking for.

How to debug the packet flow

Traffic should come in and leave the FortiGate unit. If you have determined that network traffic is not entering and leaving the FortiGate unit as expected, debug the packet flow.

Debugging can only be performed using CLI commands. Debugging the packet flow requires a number of debug commands to be entered as each one configures part of the debug action, with the final command starting the debug.

If your FortiGate unit has FortiASIC NP4 interface pairs that are offloading traffic, this will change the packet flow. Before performing the debug on any NP4 interfaces, you should disable offloading on those interfaces.

The following configuration assumes that PC1 is connected to the internal interface of the FortiGate unit and has an IP address of 10.11.101.200. PC1 is the host name of the computer.

To debug the packet flow in the CLI, enter the following commands:

```
FGT# diag debug disable
FGT# diag debug flow filter add <PC1>
FGT# diag debug flow show console enable
FGT# diag debug flow show function-name enable
FGT# diag debug flow trace start 100
FGT# diag debug enable
```

The `start 100` argument in the above list of commands will limit the output to 100 packets from the flow. This is useful for looking at the flow without flooding your log or displaying too much information.

To stop all other debug activities, enter the command:

```
FGT# diag debug flow trace stop
```

The following is an example of debug flow output for traffic that has no matching security policy, and is in turn blocked by the FortiGate unit. The denied message indicates that the traffic was blocked.

```
id=20085 trace_id=319 func=resolve_ip_tuple_fast line=2825 msg="vd-root received a packet
    (proto=6, 192.168.129.136:2854->192.168.96.153:1863) from port3."

id=20085 trace_id=319 func=resolve_ip_tuple line=2924 msg="allocate a new session-
    013004ac"

id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a route: gw-
    192.168.150.129 via port1"

id=20085 trace_id=319 func=fw_forward_handler line=248 msg=" Denied by forward policy
    check"
```

Troubleshooting resources

Before you begin troubleshooting, you need to know Fortinet's troubleshooting resources. Doing so will shorten the time to solve your issue. Indeed, an administrator can save time and effort during the troubleshooting process by first checking if the issue has been experienced before. Several self-help resources are available to provide valuable information about FortiOS technical issues, including:

Technical Documentation

Installation Guides, Administration Guides, Quick Start Guides, and other technical documents are available online at the following URL:

http://docs.fortinet.com

Fortinet Video Library

The Fortinet Video Library hosts a collection of video which provide valuable information about Fortinet products.

http://video.fortinet.com

Release Notes

Issues that are uncovered after the technical documentation has been published will often be listed in the Release Notes that accompany the device.

Knowledge Base

The Fortinet Knowledge Base provides access to a variety of articles, white papers, and other documentation providing technical insight into a range of Fortinet products. The Knowledge Base is available online at the following URL:

http://kb.fortinet.com

Fortinet Technical Discussion Forums

An online technical forums allow administrators to contribute to discussions about issues related to their Fortinet products. Searching the forum can help the administrator identify if an issue has been experienced by another user. The support forums can be accessed at the following URL:

http://forum.fortinet.com

Fortinet Training Services Online Campus

The Fortinet Training Services Online Campus hosts a collection of tutorials and training materials which can be used to increase knowledge of the Fortinet products.

http://www.fortinet.com/training/

Fortinet Customer Support

You have defined your problem, researched a solution, put together a plan to find the solution, and executed that plan. At this point if the problem has not been solved, its time to contact Fortinet Customer Support for assistance.

http://support.fortinet.com

Technical Support Organization Overview

This section explains how Fortinet's technical support works, as well as how you can easily create an account to get technical support for when issues arise that you cannot solve yourself.

This section contains the following topics:

- Fortinet Global Customer Services Organization
- Creating an account
- Registering a device
- Reporting problems
- Assisting technical support
- Support priority levels
- Return material authorization process

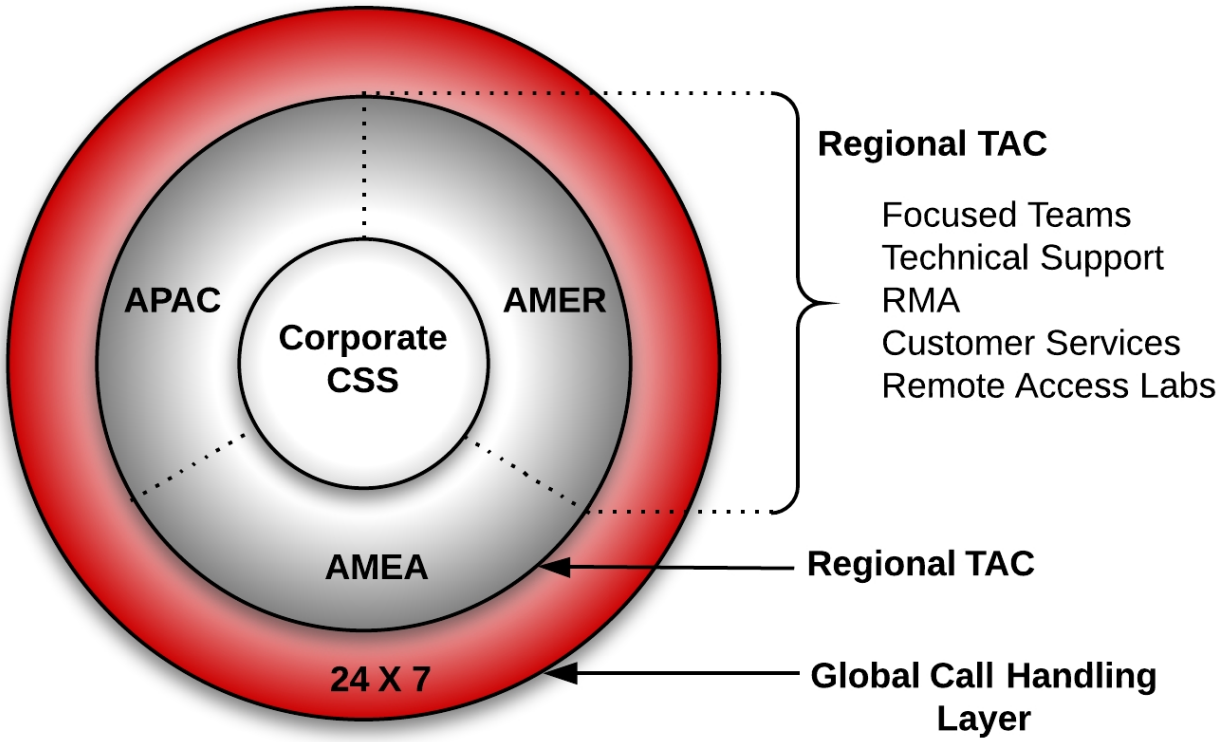
Fortinet Global Customer Services Organization

The Fortinet Global Customer Services Organization is composed of three regional **Technical Assistance Centers** (TAC):

- The Americas (AMER)
- Europe, Middle East, and Africa (EMEA)
- Asia Pacific (APAC)

The regional TACs are contacted through a global call center. Incoming service requests are then routed to the appropriate TAC. Each regional TAC delivers technical support to the customers in its regions during its hours of operation. These TACs also combine to provide seamless, around-the-clock support for all customers.

Fortinet regions and TAC



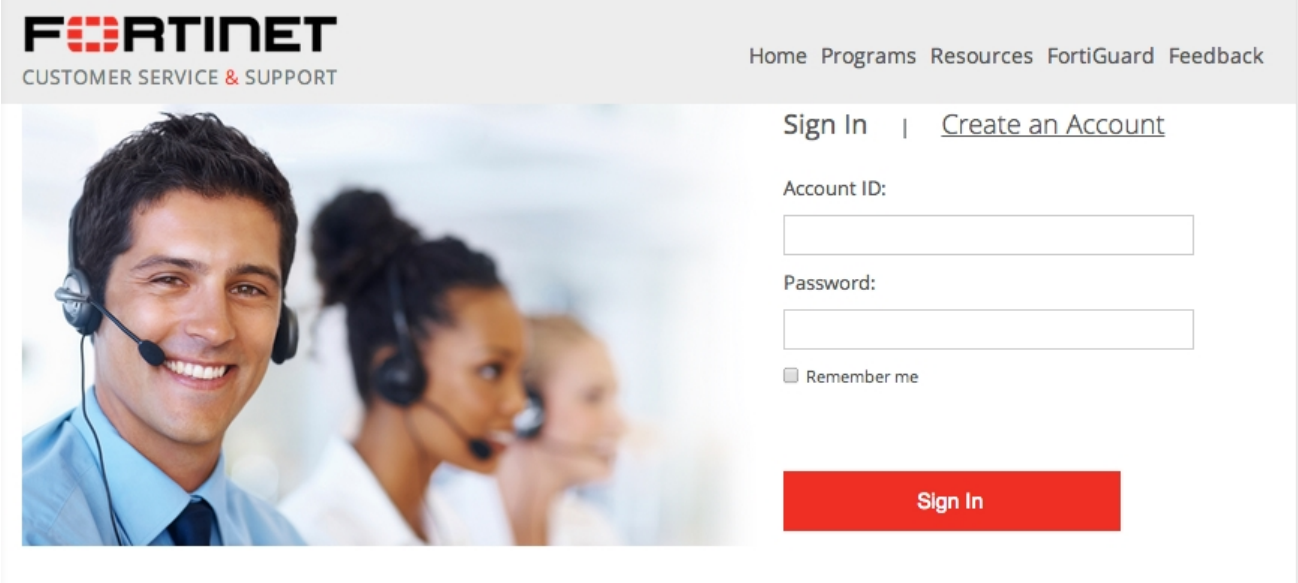
Creating an account

To receive technical support and service updates, Fortinet products in the organization must be registered. The **Product Registration Form** on the support website will allow the registration to be completed online. Creating an account on the support website is the first step in registering products.

Go to the Fortinet support site shown below:

https://support.fortinet.com/

Customer service and support home page



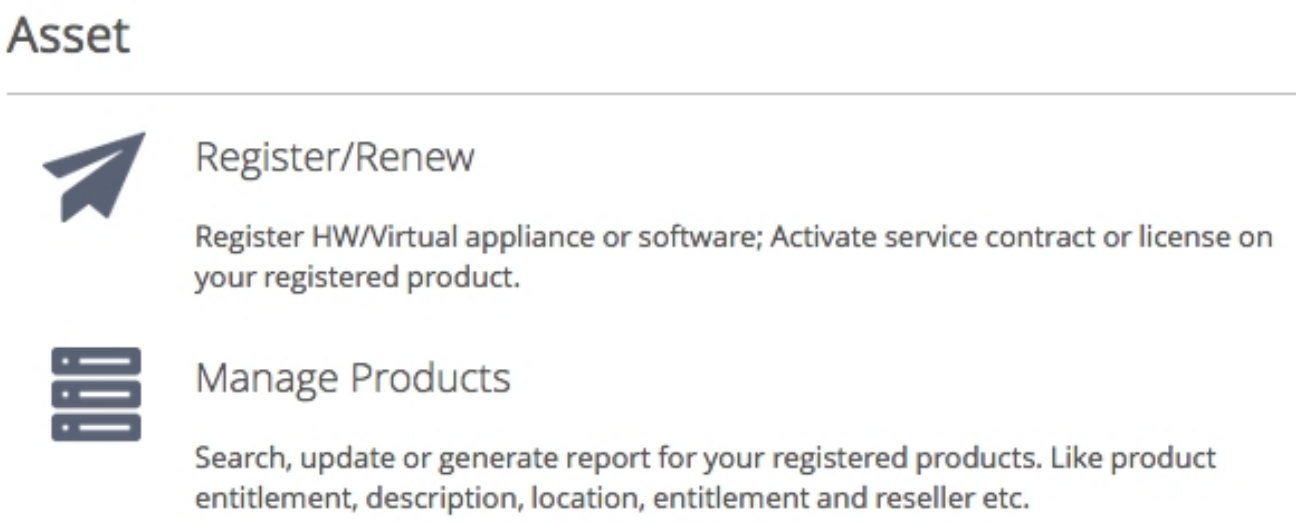
Once the support account has been created, product details can be provided by going to the **Product Register/Renew** and **Manage Product** buttons displayed on the home page. Alternately, the product registration can be completed at a later time.

Registering a device

Complete the following steps when registering a device for support purposes:

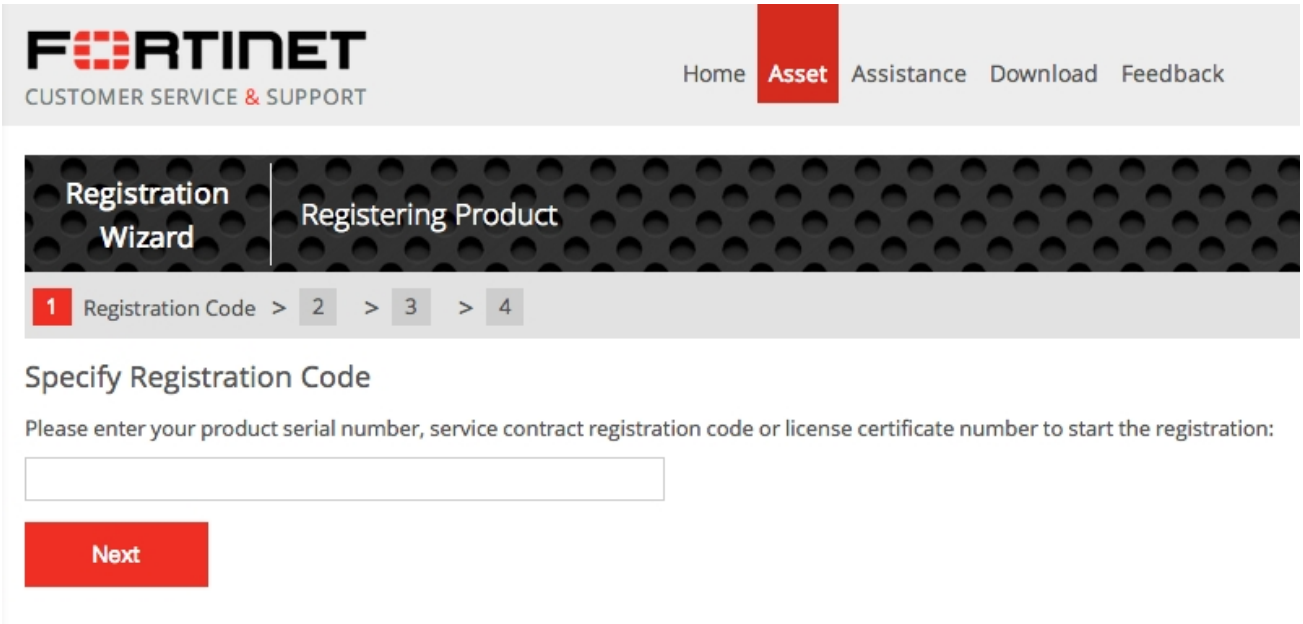
1. Log in using the **Username** and **Password** defined when the account was created
2. Under the Asset section, select **Register/Renew** to go to the Registration Wizard. Alternatively, use the Asset menu at the top of the page.

Register/Renew and Manage Products menu



3. Get a serial number from the back of the FortiGate unit or from the exterior of the FortiGate shipping box.
4. Enter the serial number, service contract registration code or license certificate number to start the product registration.

Adding a product to a support account



5. Enter your registration information.
6. Read and accept the license agreement.
7. Complete the verification process.
8. Select **Finish** to complete the registration process.
9. Registration wizard

Reporting problems

Problems can be reported to a Fortinet Technical Assistance Center in the following ways:

- By logging an online ticket
- By phoning a technical support center

Logging online tickets

Problem reporting methods differ depending on the type of customer.

Fortinet partners

Fortinet Partners are entitled to priority web-based technical support. This service is designed for partners who provide initial support to their customers and who need to open a support ticket with Fortinet on their behalf. We strongly encourage submission and follow up of support tickets using this service.

The support ticket can be submitted after logging into the partner website using one of the following links using FortiPartner account details:

http://partners.fortinet.com

This link will redirect to the general **Fortinet Partner Portal** extranet website. Click **Support** > **Online Support Ticket**.

https://forticare.fortinet.com/customersupport/Login/CommonLogin.aspx

Fortinet customers

There are two methods to report a technical issue on the Fortinet Support website: creating a technical support ticket by product or creating any type of ticket with the Ticket Wizard for more options.

Fortinet customers should complete the following steps to create a support ticket by product:

1. Log in to the support website at the following address with the account credentials used when the account was created: https://support.fortinet.com
2. Navigate to the top menu, click **Asset** and select **Manage/View Products.**
3. In the product list, select the product that is causing the problem.
4. On the left side bar, go to the Assistance category, and select **Technical Request** to create a TA Ticket.
5. Complete the **Create TA Ticket** fields.
6. Click **View Products**.
7. In the **Products List**, select the product that is causing the problem.
8. Complete the **Create Support Ticket** fields.
9. Select **Finish** to complete the support ticket.

Fortinet customers who would like to submit a customer service ticket, DOA ticket, RMA ticket, or FortiGuard service ticket should use the Ticket Wizard and complete the following steps:

1. Log in to the support website at the following address with the account credentials used when the account was created: https://support.fortinet.com

2. Navigate to the top menu, click **Assistance** and select **Create a Ticket** from the drop down menu.
3. Select a ticket type and complete the remaining steps in the Ticket Wizard.
4. Select **Finish** to complete the ticket.

Following up on online tickets

Perform the following steps to follow up on an existing issue.

Partners should log into the following web site:

http://partners.fortinet.com

Customers should log into the following site:

http://support.fortinet.com

1. Log in with the account credentials used when the account was created.
2. Navigate to the top menu, click **Assistance**, and select **Manage Tickets**.
3. Use the search field on the View Tickets page to locate the tickets assigned to the account.
4. Select the appropriate ticket number. Closed tickets cannot be updated. A new ticket must be submitted if it concerns the same problem.
5. Add a **New Comment** or **Attachment**.
6. Click **Submit** when complete.

Every web ticket update triggers a notification to the ticket owner, or ticket queue supervisor.

Telephoning a technical support center

The Fortinet Technical Assistance Centers can also be contacted by phone.

Call Fortinet Support Center at 1-408-486-7899 (international) or go to http://www.fortinet.com/support/contact_support.html and select your country from the drop-down list for local contact number.

Assisting technical support

The more information that can be provided to Fortinet technical support, the better they can assist in resolving the issue. Every new support request should contain the following information:

- A valid contact name, phone number, and email address.
- A clear and accurate problem description.
- A detailed network diagram with complete IP address schema.
- The configuration file, software version, and build number of the Fortinet device.
- Additional log files such as **Antivirus** log, **Attack** log, **Event** log, **Debug** log or similar information to include in the ticket as an attachment. If a third-party product is involved, for example, email server, FTP server, router, or switch, please provide the information on its software revision version, configuration, and brand name.

Support priority levels

Fortinet technical support assigns the following priority levels to support cases:

Priority 1

This **Critical** priority is assigned to support cases in which:

- The network or system is down causing customers to experience a total loss of service.
- There are continuous or frequent instabilities affecting traffic-handling capability on a significant portion of the network.
- There is a loss of connectivity or isolation to a significant portion of the network.
- This issue has created a hazard or an emergency.

Priority 2

This **Major** priority is assigned to support cases in which:

- The network or system event is causing intermittent impact to end customers.
- There is a loss of redundancy.
- There is a loss of routine administrative or diagnostic capability.
- There is an inability to deploy a key feature or function.
- There is a partial loss of service due to a failed hardware component.

Priority 3

This **Medium** priority is assigned to support cases in which:

- The network event is causing only limited impact to end customers.
- Issues seen in a test or pre-production environment exist that would normally cause adverse impact to a production network.
- The customer is making time sensitive information requests.
- There is a successful workaround in place for a higher priority issue.

Priority 4

This **Minor** priority is assigned to support cases in which:

- The customer is making information requests and asking standard questions about the configuration or functionality of equipment.

Customers must report Priority 1 and 2 issues by phone directly to the Fortinet EMEA Support Center.

For lower priority issues, you may submit an assistance request (ticket) via the web system.

The web ticket system also provides a global overview of all ongoing support requests.

Return material authorization process

In some cases hardware issues are experienced and a replacement unit must be sent. This is referred to as a Return Material Authorization (RMA). In these cases or RMAs, the support contract must be moved to the new device. Customers can move the support contract from the failing production unit to the new device through the support web site.

To move the support contract to a new device

1. Log in to the support web site with the credentials indicated when the account was created.
2. From **Manage Products**, locate the serial number of the defective unit from the list of devices displayed for the account. The **Product Info** for the selected device will be displayed.
3. In the left side bar under the **Assistance section**, select **RMA Transfer**.
4. Enter the **Original Serial Number** of the original device, enter the **New Serial Number,** and click **Replace** to complete the transfer.

This will transfer the support contract from the defective unit to the new unit with the serial number provided.

Chapter 27 - Virtual Domains

This FortiOS Handbook chapter contains the following sections:

Virtual Domains provides an overview of the VDOM technologies, and the basic concepts and rules for using them. We recommend that you begin with this chapter before attempting to configure VDOMs on your FortiGate unit.

Virtual Domains in NAT/Route mode on page 2577 provides detailed explanations and examples for configuring VDOM features in your FortiGate unit using the NAT/Route mode.

Virtual Domains in Transparent mode on page 2596 provides detailed explanations, as well as basic and advanced examples for configuring these features in your FortiGate unit using Transparent mode.

Inter-VDOM routing on page 2615 describes inter-VDOM routing concepts and scenarios, and gives examples that illustrate them.

Troubleshooting Virtual Domains on page 2652 provides diagnostic and troubleshooting information for some potential VDOM issues.

Virtual Domains

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate firewall policies and, in NAT/Route mode, completely separate configurations for routing and VPN services for each connected network or organization.

This chapter will cover the basics of VDOMs, how they change your FortiGate unit, and how to work with VDOMs.

VDOMs let you split your physical FortiGate unit into multiple virtual units. The resulting benefits range from limiting Transparent mode ports to simplified administration, to reduced space and power requirements.

When VDOMs are disabled on any FortiGate unit, there is still one VDOM active: the root VDOM. It is always there in the background. When VDOMs are disabled, the root VDOM is not visible but it is still there.

The root VDOM must be there because the FortiGate unit needs a management VDOM for management traffic among other things. It is also why when you enable VDOMs, all your configuration is preserved in the root VDOM- because that is where you originally configured it.

This section includes:

- Benefits of Virtual Domains
- Enabling and accessing Virtual Domains
- Configuring Virtual Domains

Benefits of Virtual Domains

VDOMs provide the following benefits:

- Improving Transparent mode configuration
- Easier administration
- Continued security
- Savings in physical space and power
- More flexible MSSP configurations

Improving Transparent mode configuration

When VDOMs are not enabled and you put your FortiGate unit into Transparent mode, all the interfaces on your unit become broadcast interfaces. The problem with this is that there are no interfaces free to do anything else.

With multiple VDOMs you can have one of them configured in Transparent mode, and the rest in NAT/Route mode. In this configuration, you have an available transparent mode FortiGate unit you can drop into your network for troubleshooting, and you also have the standard NAT for networking.

Easier administration

VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. VDOMs separate security domains and simplify administration of complex configurations—you do not have to manage as many settings at one time. For more information, see Global and per-VDOM settings.

By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the unit's physical interfaces, modem, VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings.

Also, you can optionally assign an administrator account restricted to one VDOM. If the VDOM is created to serve an organization, this feature enables the organization to manage its own configuration. For more information, see Administrators in Virtual Domains.

Each physical FortiGate unit requires a FortiGuard license to access security updates. VDOMs do not require any additional FortiGuard licenses, or updating — all the security updates for all the VDOMs are performed once per update at the global level. Combined this can be a potentially large money and time saving feature in your network.

Management systems such as SNMP, logging, alert email, FDN-based updates, and NTP-based time setting use addresses and routing in the management VDOM to communicate with the network. They can connect only to network resources that communicate with the management VDOM. Using a separate VDOM for management traffic enables easier management of the FortiGate unit global settings, and VDOM administrators can also manage their VDOMs more easily. For more information, see Changing the management virtual domain.

Continued security

When a packet enters a VDOM, it is confined to that VDOM and is subject to any firewall policies for connections between VLAN subinterfaces or zones in that VDOM, just like those interfaces on a FortiGate unit without VDOMs enabled.

To travel between VDOMs, a packet must first pass through a firewall policy on a physical interface. The packet then arrives at another VDOM on that same FortiGate unit, but on a different interface, where it must pass through another firewall before entering. It doesn't matter if the interface is physical or virtual — inter-VDOM packets still require the same security measures as when passing through physical interfaces.

VDOMs provide an additional level of security because regular administrator accounts are specific to one VDOM — an administrator restricted to one VDOM cannot change information on other VDOMs. Any configuration changes and potential errors will apply only to that VDOM and limit any potential down time. Using this concept, you can farther split settings so that the management domain is only accessible by the super_admin and does not share any settings with the other VDOMs.

Savings in physical space and power

To increase the number of physical FortiGate units, you need more rack space, cables, and power to install the new units. You also need to change your network configuration to accommodate the new physical units. In the future, if you need fewer physical units you are left with expensive hardware that is idle.

Increasing VDOMs involves no additional hardware, no additional cabling, and very few changes to existing networking configurations. VDOMs save physical space and power. You are limited only by the size of the VDOM license you buy and the physical resources on the FortiGate unit.

By default, FortiGate units support a maximum of 10 VDOMs in any combination of NAT/Route and Transparent modes. Many FortiGate models support purchasing a license key to increase the maximum number. For more information on VDOM licences, see Virtual Domain Licensing.

More flexible MSSP configurations

If you are a managed security and service provider (MSSP), VDOMs are fundamental to your business. As a service provider you have multiple customers, each with their own needs and service plans. VDOMs allow you to

have a separate configuration for each customer, or group of customers; with up to 500 VDOMs configured per FortiGate unit on high end models. See Virtual Domain Licensing.

Not only does this provide the exact level of service needed by each customer, but administration of the FortiGate unit is easier as well - you can provide uninterrupted service generally with immediate changes as required. Most importantly, it allows you to only use the resources that each customer needs. Inter-VDOM links allow you to customize the level of interaction you need between each of your customers and your administrators. See Inter-VDOM routing.

Enabling and accessing Virtual Domains

While Virtual Domains are essentially the same as your regular FortiGate unit for menu configuration, CLI command structure, and general task flow, there are some small differences.

After first enabling VDOMs on your FortiGate unit, you should take the time to familiarize yourself with the interface. This section will help walk you through virtual domains.

This section includes:

- Enabling Virtual Domains
- Viewing the VDOM list
- Global and per-VDOM settings
- Resource settings
- Virtual Domain Licensing
- Logging in to VDOMs

Enabling Virtual Domains

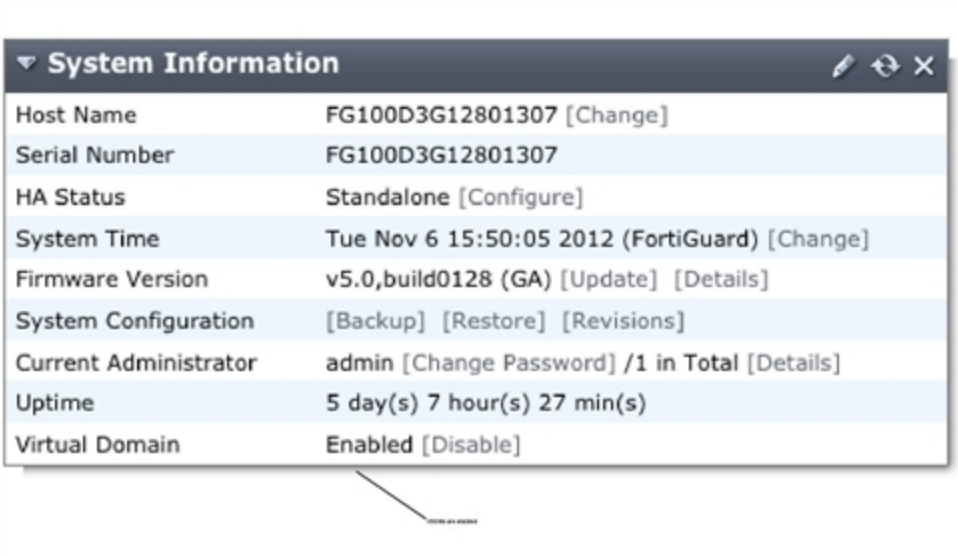
Using the default admin administration account, you can enable or disable VDOM operation on the FortiGate unit.

To enable VDOM configuration - web-based manager:

1. Log in with a super_admin account.
2. Go to **System > Dashboard > Status**.
3. Under **System Information > Virtual Domain**, select **Enable** and confirm your selection.

The FortiGate unit logs off all sessions. You can now log in again as admin. For more information, see Administrators in Virtual Domains.

System Information



To enable VDOM configuration - CLI:

```
config system global
   set vdom-admin enable
end
```

Changes to the web-based manager and CLI

When Virtual Domains are enabled, your FortiGate unit will change. The changes will be visible in both the web-based manager and CLI, just the web-based manager, or just the CLI.

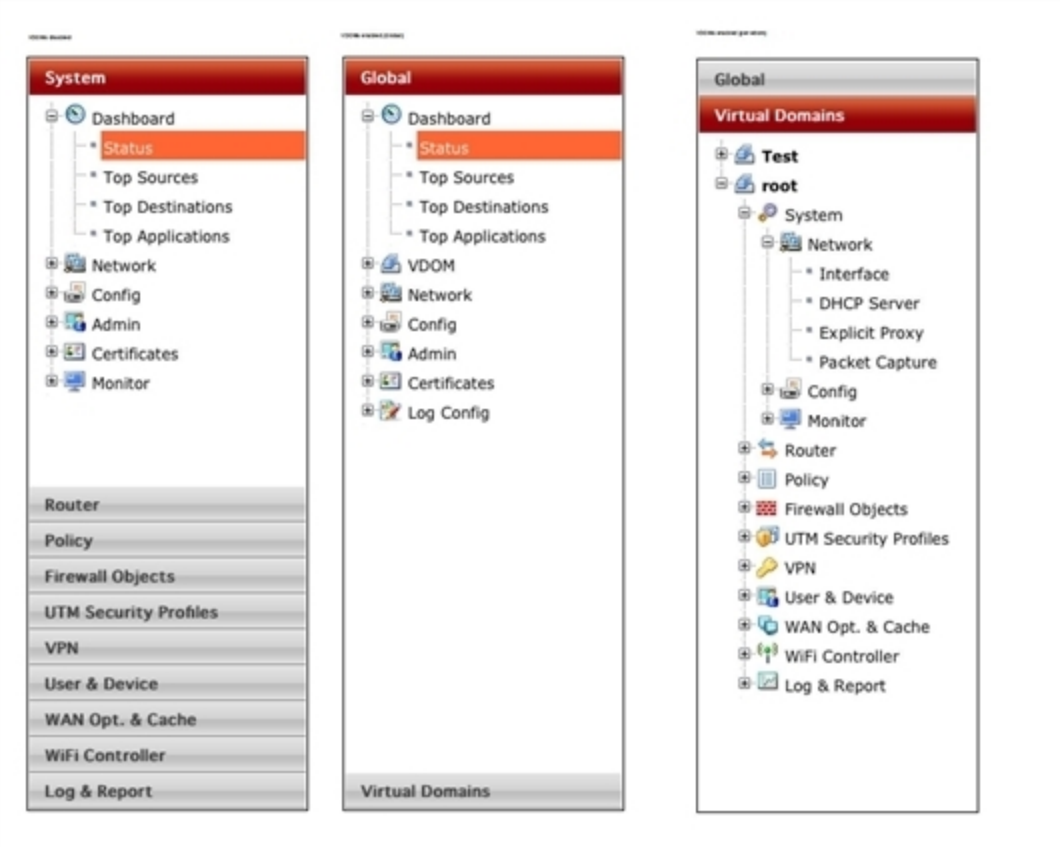
When enabling VDOMs, the web-based manager and the CLI are changed as follows:

- Global and per-VDOM configurations are separated. This is indicated in the Online Help by Global and VDOM icons. See Global and per-VDOM settings.
- Only admin accounts using the super_admin profiles can view or configure global options. See Administrators in Virtual Domains.
- Admin accounts using the super_admin profile can configure all VDOM configurations.
- All other administrator accounts can configure only the VDOM to which they are assigned.

The following changes are specific to the web-based manager:

- In the Global view, the System section of the left-hand menu is renamed to Global, and includes a VDOM sub-menu.
- The Log Config menu is moved from Log & Report into the new Global section.
- For admin accounts using the super_admin profile, a new section called Virtual Domains is added at the bottom of the left-hand menu. It lists all the individual VDOMs as expandable menus, with all VDOM specific options in that menu, which allows you to easily select which VDOM to configure, including the root VDOM. See Menu with VDOMs disabled, at the global level, and VDOM level.

Menu with VDOMs disabled, at the global level, and VDOM level



In the CLI, admin accounts using the super_admin profile must specify either the global or a VDOM-specific shell before entering commands:

- To change FortiGate unit system settings, from the top level you must first enter the following CLI before entering commands:

  ```
  config global
  ```

- To change VDOM settings, from the top level you must first enter the following CLI before entering commands for that VDOM:

  ```
  config vdom
     edit <vdom_na
  ```

Settings configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus settings, and some logging settings. In general, any unit settings that should only be changed by the top level administrator are global settings.

Settings configured configwithin a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging, and reporting.

For more information, see Global and per-VDOM settings.

Viewing the VDOM list

The VDOM list shows all virtual domains, their status, and which VDOM is the management VDOM. It is accessible if you are logged in on an administrator account with the super_admin profile such as the “admin” administrator account.

In the VDOM list you can create or delete VDOMs, edit VDOMs, change the management VDOM, and enable or disable VDOMs.

You can access the VDOM list in **Global > VDOM > VDOM**.

The root domain cannot be disabled, even if it is not the management VDOM.

List of VDOMs

Create New	Select to add a new VDOM. See Creating a Virtual Domain.
Edit	Select to change an existing selected VDOM.
Delete	Select to delete the selected VDOM. See Deleting a VDOM.
Switch Management	Select to switch the management VDOM. Also shows the current management VDOM. You must select an active non-management VDOM before this option becomes available. See Changing the management virtual domain.
Selected	When checked, this checkbox indicates this VDOM has been selected. Nearly all operations such as Edit, Delete, and Switch Management require a VDOM to first be selected.
Name	The name of the VDOM. VDOMs are listed in alphabetical order. When the VDOM is active, you can select the VDOM name to enter that VDOM. See Enabling and accessing Virtual Domains.
Operation Mode	Indicates the operation mode as either NAT (for NAT/Route mode) or TP (for Transparent mode).
Interfaces	The interfaces associated with this VDOM. Each VDOM also includes an interface that starts with “ssl.” that is created by default.
Enable	A green checkmark indicates this VDOM is active. See Disabling a Virtual Domain. A grey X indicated this VDOM is disabled. See Disabling a Virtual Domain.
Comments	Comments entered when the VDOM was created are displayed here.
Ref.	The number of references to this VDOM in the configuration.

Global and per-VDOM settings

Settings configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus, and some logging. In general, any unit settings that should only be changed by the top level administrator are global settings.

Settings configured within a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging settings, and reporting.

When Virtual Domains are not enabled, the entire FortiGate unit is effectively a single VDOM. Per-VDOM limits apply. For some resource types, the global limit cannot be reached with only one VDOM.

Some FortiGate unit documentation indicates which parts of the web-based manager, or the CLI are global and which are per-VDOM using the icons shown below. These icons are also present in the Online Help, available on your FortiGate unit.

Global and VDOM icons

For more information on CLI commands, see the FortiGate CLI Reference.

This section includes:

- Global settings - web-based manager
- Per-VDOM settings - web-based manager
- Global settings - CLI
- Per-VDOM settings - CLI

Global settings - web-based manager

The following table lists commands in the web-based manager that are considered global settings when VDOMs are enabled.

The following configuration settings affect all virtual domains. When virtual domains are enabled, only accounts with the default super_admin profile can access global settings.

Global configuration settings

System	Dashboard > Status - Host name
	Dashboard > Status - HA Status
	Dashboard > Status - System Time
	Dashboard > Status - Firmware version
	Dashboard > Status - Configuration backup and restore
	VDOM > VDOM - list
	VDOM > VDOM - edit VDOM (mode and resources)
	VDOM > Global Resources
	Network > Interfaces
	Network > DNS - DNS and DDNS settings
	Config > HA
	Config > SNMP
	Config > Replacement Message - messages and images
	Config > FortiGuard - configuration
	Config > Advanced - scripts, USB Auto-install, debug log download
	Config > Messaging Servers
	Admin > Administrators
	Admin > Admin Profile
	Admin > Settings - web administration ports, password policy, display settings, timeouts, LCD panel
	Certificates - local, remote, and CA certificates, CRLs
Log&Report	Log Config - Log Setting

Per-VDOM settings - web-based manager

The following table lists commands in the web-based manager that are considered per-VDOM settings when VDOMs are enabled.

VDOM configuration settings

System	Dashboard > Status - read-only except for administrator password
	Network > Interfaces (and zones)
	Network > DHCP Server
	Network > Explicit Proxy
	Network > Routing Table (Transparent mode only)
	Network > Packet Capture
	Config > Replacement Message (messages and images)
	Config > Advanced
	Monitor > DHCP Monitor
Router	All settings, including dead gateway detection
Policy	All settings
Firewall Objects	All settings
Security Profiles	All settings
VPN	All settings
User & Device	All settings
WiFi Controller	All settings
Log&Report	Traffic and Event Logs
	Reports
	FortiCloud
	Log Config > Log Setting and Alert E-mail
	Logging Monitor

Global settings - CLI

The following table lists commands in the CLI that are considered global settings when VDOMs are enabled.

From a super_admin profile account, use this command to configure features that apply to the complete FortiGate unit including all virtual domains. Virtual domain configuration (vdom-admin) must be enabled first.

This command syntax shows how you access the commands within config global. For information on these commands, refer to the relevant sections in the CLI Reference. If there are multiple versions of the same command with a “2” or “3” added, the additional commands are not listed but fall under the unnumbered command of the same name.

```
config global
   config antivirus heuristic
   config antivirus service
   config application name
   config dlp settings
   config endpoint-control app-detect
   config firewall ssl
   config gui console
   config ips decoder
   config ips global
   config ips rule
   config log fortianalyzer setting
   config log fortiguard setting
   config log memory global-setting
   config log syslogd filter
   config log syslogd setting
   config log webtrends ...
   config spamfilter fortishield
   config spamfilter options
   config system accprofile
   config system admin
   config system auto-install
   config system autoupdate ...
   config system bug-report
   config system central-management
   config system chassis-loadbalance
   config system console
   config system custom-language
   config system ddns
   config system dedicated-mgmt
   config system dns
   config system dscp-based-priority
   config system email-server
   config system fips-cc
   config system fortiguard
   config system fortisandbox
   config system fsso-polling
   config system geoip-override
   config system global
   config system ha
   config system interface
   config system ips-urlfilter-dns
   config system lte-modem
   config system netflow
```

```
config system npu
config system ntp
config system password-policy
config system physical-switch
config system probe-response
config system replacemsg ...
config system replacemsg-image
config system resource-limits
config system session-helper
config system session-sync
config system sflow
config system sms-server
config system snmp ...
config system storage
config system switch-interface
conifg system tos-based-priority
config system vdom-link
config system vdom-property
config system vdom-radius-server
config system virtual-switch
config vpn certificate ...
config wanopt storage
config webfilter fortiguard
config webfilter ips-urlfilter-cache-setting
config wireless-controller global
config wireless-controller timers
config wireless-controller vap
execute FortiClient-NAC
execute backup
execute batch
execute central-mgmt
execute cfg reload
execute cfg save
execute cli check-template-status
execute cli status-msg-only
execute date
execute disconnect-admin-session
execute disk
execute enter
execute erase-disk
execute extender
execute factoryreset
execute factoryreset2
execute formatlogdisk
execute forticlient
execute fortiguard-log
execute fortiguard-message
execute ha ignore-hardware-revision
execute log ...
execute policy-packet-capture
execute reboot
execute report-config
execute restore
execute revision
execute router clear
execute send-fds-statistics
execute set system
```

```
execute set-next-reboot
execute sfp-mode-sgmii
execute shutdown
execute switch-controller
execute system
execute tac
execute time

execute update-av
execute update-geo-ip
execute update-ips
execute update-list
execute update-netscan
execute update-now
execute update-src-vis
execute upload
execute usb-disk
execute vpn certificate ...
execute wireless-controller delete-wtp-image
execute wireless-controller list-wtp-image
execute wireless-controller restart-acd
execute wireless-controller upload-wtp-image
get antivirus heuristic
get application name
get dlp settings
get endpoint-control forticlient-registration-sync
get extender modem-status
get extender sys-info
get firewall ipv6-eh-filter
get firewall ssl
get gui console
get hardware cpu
get hardware memory
get hardware nic
get hardware npu
get hardware status
get ips decoder
get ips global
get ips rule
get ips view-map
get log fortianalyzer
get log fortguard
get log memory
get log syslog
get webtrends
get mgmt-data status
get spamfilter fortishield
get spamfilter options
get system accprofile
get system admin
get system auto-install
get system auto-update
get system autoupdate
get system central-management
get system central-mgmt
get system checksum
get system cmdb
```

```
get system console
get system custom-language
get system ddns
get system dedicated-mgmt
get system dns
get system dscp-based-priority
get system email-server
get system fips-cc
get system fortianalyzer-connectivity
get system fortiguard
get system fortiguard-log-service
get system fortiguard-service
get system fortisandbox
get system fsso-polling
get system geoip-country
get system geoip-override
get system global
get system ha
get system ha-nonsync-csum
get system info
get system interface
get system ips-urlfilter-dns
get system lte-modem
get system mgmt-csum
get system netflow
get system npu
get system ntp
get system password-policy
get system performance
get system physical-switch
get system probe-response
get system replacemsg
get system replacemsg-image
get system resource-limits
get system session-helper
get system session-helper-info
get system session-info
get system session-sync
get system sflow
get system sms-server
get system snmp
get system source-ip
get system startup-error-log
get system status
get system storage
get system switch-interface
get system tos-based-priority
get system vdom-link
get system vdom-property
get system vdom-radius-server
get system virtual-switch
get test <name of daemon>
get user device-category
get vpn certificate
get wanopt storage
get webfilter fortiguard
get webfilter ftgd-statistics
```

```
    get webfilter ips-urlfilter-cache-setting
    get webfilter status
    get wireless-controller client-info
    get wireless-controller global
    get wireless-controller rf-analysis
    get wireless-controller scan
    get wireless-controller spectral-info
    get wireless-controller status
    get wireless-controller timers
    get wireless-controller vap
    get wireless-controller vap-status
    get wireless-controller wtp-status
end
```

Per-VDOM settings - CLI

The following table lists commands in the CLI that are considered VDOM-specific settings when VDOMs are enabled.

From the super_admin account, you can use the commands below to add and configure virtual domains. The number of virtual domains you can add is dependent on the FortiGate model. Virtual domain configuration (vdom-admin) must be enabled.

Once you add a virtual domain you can configure it by adding zones, firewall policies, routing settings, and VPN settings. You can also move physical interfaces from the root virtual domain to other virtual domains and move VLAN subinterfaces from one virtual domain to another.

By default all physical interfaces are in the root virtual domain. You cannot remove an interface from a virtual domain if the interface is part of any of the following configurations:

- routing
- proxy arp
- DHCP server
- zone
- firewall policy
- redundant pair
- link aggregate (802.3ad) group

Delete these objects, or modify them, to be able to remove the interface.

This command syntax shows how you access the commands within a VDOM. Refer to the relevant sections in this Reference for information on these commands.

```
config vdom
   edit <vdom_name>
      config antivirus profile
      config antivirus quarantine
      config antivirus settings
      config application list
      config application rule-settings
      config dlp filepattern
      config dlp fp-doc-source
      config dlp fp-sensitivity
      config dlp sensor
      config endpoint-control profile
      config endpoint-control settings
```

```
config firewall ... (except ssl)
config ftp-proxy
config icap
config imp2p aim-user
config imp2p icq-user
config imp2p msn-user
config imp2p old-version
config imp2p policy
config imp2p yahoo-user
config ips custom
config ips rule-settings
config ips sensor
config ips settings
config log custom-field
config log disk
config log eventfilter
config log fortianalyzer
config log fortiguard
config log memory
config log setting
config log syslogd
config netscan
config router
config spamfilter bwl
config spamfilter bword
config spamfilter dnsbl
config spamfilter iptrust
config spamfilter mheader
config spamfilter profile
config system 3g-modem
config system admin
config system arp-table
config system dhcp ...
config system dhcp6 ...
config system dns-database
config system dns-server
config system gre-tunnel
config system interface
config system ipip-tunnel
config system ipv6-neighbor-cache
config system ipv6-tunnel
config system modem ..
config system monitors
config system nat64
config sysetm network-visibility
config system object-tag
config system proxy-arp
config system replacemsg-group
config system server-probe
config system session-ttl
config system settings
config system sit-tunnel
config system switch-interface
config system wccp
config system zone
config user ...
config voip
```

```
config vpn ...
config wanopt auth-group
config wanopt peer
config wanopt profile
config wanopt settings
config wanopt ssl-server
config wanopt webcache
config web-proxy debug-url
config web-proxy explicit
config web-proxy forward-server
config web-proxy forward-server-group
config web-proxy global
config web-proxy url-match
config webfilter content
config webfilter content-header
config webfilter ftgd-local-cat
config webfilter ftgd-local-rating
config webfilter ftgd-local-warning
config webfilter ips-urlfilter-setting
config webfilter override
config webfilter override-user
config webfilter profile
config webfilter search-engine
config webfilter urlfilter
config wireless-controller ap-status
config wireless-controller setting
config wireless-controller vap
config wireless-controller sids-profile
config wireless-controller wtp
config wireless-controller wtp-profile
execute backup
execute clear system arp table
execute cli check-template-status
execute cli status-msg-only
execute client-reputation
execute dhcp lease-clear
execute dhcp lease-list
execute dhcp6 lease-clear
execute dhcp6 lease-list
execute enter
execute fortitoken ...
execute fortitoken-mobile
execute fsso refresh
execute interface dhcpclient-renew
execute interface pppoe-reconnect
execute log ...
execute log-report reset
execute modem dial
execute modem hangup
execute modem trigger
execute mrouter clear
execute netscan ...
execute ping, ping6
execute ping-options, ping6-options
execute policy-packet-capture
execute report
execute report-config
```

```
      execute restore
      execute revision
      execute router clear
      execute sfp-mode-sgmii
      execute ssh
      execute switch-controller
      execute tac
      execute telnet
      execute traceroute
      execute tracert6
      execute upload
      execute usb-device
      execute usb-disk
      execute vpn ipsec tunnel
      execute vpn sslvpn ...
      execute wireless-controller reset-wtp
   next
   edit <another_vdom>
      config ...
      execute ...
   end
```

For more information, see Global and per-VDOM settings.

Resource settings

Your FortiGate unit has a limited amount of hardware resources such as memory, disk storage, CPU operations. When Virtual Domains are disabled, this limit is not a major concern because all sessions, users, and other processes share all the resources equally.

When using Virtual Domains, hardware resources can be divided differently between Virtual Domains as they are needed. Minimum levels of resources can be specified for each VDOM, so that no Virtual Domain will suffer a complete lack of resources.

For example, if one VDOM has only a web server and logging server connected, and a second VDOM has an internal network of 20 users, these two VDOMs will require different levels of resources. The first VDOM will require many sessions but no user accounts. This compares to the second VDOM where user accounts and management resources are required, but fewer sessions.

Using the global and per-VDOM resource settings, you can customize the resources allocated to each VDOM to ensure the proper level of service is maintained on each VDOM.

This section includes:

- Global resource settings
- Per-VDOM resource settings

Global resource settings

Global Resources apply to the whole FortiGate unit. They represent all of the hardware capabilities of your unit. By default the values are set to their maximum values. These values vary by your model due to each model having differing hardware capabilities.

It can be useful to change the maximum values for some resources to ensure there is enough memory available for other resources that may be more important to your configuration.

To use the earlier example, if your FortiGate unit is protecting a number of web servers and other publicly accessible servers you would want to maximize the available sessions and proxies while minimizing other settings that are unused such as user settings, VPNs, and dial-up tunnels.

Global Resources are only configurable at the global level, and only the admin account has access to these settings.

Note that global resources, such as the log disk quota resource, will only be visible if your FortiGate unit hardware supports those resources, such as having a hard disk to support the log disk resource.

Global Resources- web-based manager

Edit Reset to default value

Resource	Configured Maximum	Default Maximum	Current Usage
Sessions	0	0	26
VPN IPsec Phase1 Tunnels	10000	10000	0
VPN IPsec Phase2 Tunnels	10000	10000	0
Dial-up Tunnels	0	0	0
Firewall Policies	100000	100000	3
Firewall Addresses	20000	20000	11
Firewall Address Groups	10000	10000	0
Firewall Custom Services	0	0	0
Firewall Service Groups	0	0	0
Firewall One-time Schedules	0	0	0
Firewall Recurring Schedules	0	0	5
Local Users	0	0	0
User Groups	0	0	0
SSL VPN	0	0	0
Concurrent web proxy users	2000	2000	0
log disk quota	0	0	0

To view global resource settings - web-based manager:

1. Select **Global > VDOM > Global Resources**.
   The following information is displayed:

Edit	Select to edit the **Configured Maximum** value for a single selected **Resource**. If multiple **Resources** are selected, **Edit** is not available.
Reset to default value	Select to return one or more selected **Resources** to factory default settings.
Checkbox	Select a **Resource** for editing or resetting to default values.
Resource	The name of the available global resources.
Configured Maximum	The currently configured maximum for this resource. This value can be changed by selecting the **Resource** and editing it.
Default Maximum	The factory configured maximum value for this resource. You cannot set the **Configured Maximum** higher than the **Default Maximum**.

Current Usage	The amount of this resource that is currently being used. This value is useful for determining when and if you may need to adjust **Configured Maximum** values for some resources on your FortiGate unit.

To view global resource settings - CLI:

```
config global
   config system resource-limits
   get
```

When viewing the global resource limits in the CLI, the output appears similar to:

```
FGT1000A (global) # config system resource-limits
FGT1000A (resource-limits) # get

session : 0
ipsec-phase1 : 10000
ipsec-phase2 : 10000
dialup-tunnel : 0
firewall-policy : 100000
firewall-address : 20000
firewall-addrgrp : 10000
custom-service : 0
service-group : 0
onetime-schedule : 0
recurring-schedule : 0
user : 0
user-group : 0
sslvpn : 0
proxy : 2000
```

For explicit proxies, when configuring limits on the number of concurrent users, you need to allow for the number of users based on their authentication method. Otherwise you may run out of user resources prematurely.

Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSAE, local database etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.

For all other situations, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.

Per-VDOM resource settings

While Global resources apply to resources shared by the whole FortiGate unit, per-VDOM resources are specific to only one Virtual Domain.

By default all the per-VDOM resource settings are set to no limits. This means that any single VDOM can use up all the resources of the entire FortiGate unit if it needs to do so. This would starve the other VDOMs for resources to the point where they would be unable to function. For this reason, it is recommended that you set some maximums on resources that are most vital to your customers.

Each Virtual Domain has its own resource settings. These settings include both maximum, and minimum levels. The maximum level is the highest amount of that resource that this VDOM can use if it is available on the FortiGate unit. Minimum levels are a guaranteed level that this minimum level of the resource will always be available no matter what the other VDOMs may be using.

Figure 6: Per-VDOM resources - web-based manager:

Resource Usage

Resource	Maximum	Guaranteed	Current
Sessions	0	0	24
VPN IPsec Phase1 Tunnels	0	0	0
VPN IPsec Phase2 Tunnels	0	0	0
Dial-up Tunnels	0	0	0
Firewall Policies	0	0	3
Firewall Addresses	0	0	3
Firewall Address Groups	0	0	0
Firewall Custom Services	0	0	0
Firewall Service Groups	0	0	0
Firewall One-time Schedules	0	0	0
Firewall Recurring Schedules	0	0	1
Local Users	0	0	0
User Groups	0	0	0
SSL VPN	0	0	0
Concurrent web proxy users	0	0	0
log disk quota	0	0	0

For example, consider a FortiGate unit that has ten VDOMs configured. vdom1 has a maximum of 5000 sessions and a minimum of 1000 sessions. If the FortiGate unit has a global maximum of 20,000 sessions, it is possible that vdom1 will not be able to reach its 5000 session upper limit. However, at all times vdom1 is guaranteed to have 1000 sessions available that it can use. On the other hand, if the remaining nine VDOMs use only 1000 sessions each, vdom1 will be able to reach its maximum of 5000.

To view per-VDOM resource settings - web-based manager:

1. Select **Global > VDOM > VDOM**.
2. Select the `root` VDOM, and select **Edit**.
3. Adjust the settings in the **Resource Usage** section of the page.

Resource	Name of the resource. Includes dynamic and static resources.
Maximum	Override the global limit to reduce the amount of each resource available for this VDOM. The maximum must be the same as or lower than the global limit. The default value is 0, which means the maximum is the same as the global limit. **Note:** If you set the maximum resource usage for a VDOM you cannot reduce the default maximum global limit for all VDOMs below this maximum.
Guaranteed	Enter the minimum amount of the resource available to this VDOM regardless of usage by other VDOMs. The default value is 0, which means that an amount of this resource is not guaranteed for this VDOM.
Current	The amount of the resource that this VDOM currently uses.

4. Select **OK**.

To view per-VDOM resource settings - CLI:

```
config global
   config system vdom-property
      edit root
   get
```

When viewing the per-VDOM resource limits in the CLI, the output appears similar to the following. Note that the first two lines are not part of the resource limits. In the CLI, the first number is the maximum value, and the second number is the guaranteed minimum.

```
FGT1KA3607500810 (vdom-property) # edit root
FGT1KA3607500810 (root) # get

name : root
description : property limits for vdom root
session : 0 0
ipsec-phase1 : 0 0
ipsec-phase2 : 0 0
dialup-tunnel : 0 0
firewall-policy : 0 0
firewall-address : 0 0
firewall-addrgrp : 0 0
custom-service : 0 0
service-group : 0 0
onetime-schedule : 0 0
recurring-schedule : 0 0
user : 0 0
user-group : 0 0
```

```
sslvpn : 0 0
proxy : 0 0
```

Virtual Domain Licensing

Many FortiGate models support purchasing a license key to increase the maximum number. For specific information about the number of VDOM licenses that your FortiGate supports, see the product data sheet.

Configuring 500 or more VDOMs will result in reduced system performance. See FortiGate unit running very slowly.

Your FortiGate unit has limited resources that are divided among all configured VDOMs. These resources include system memory and CPU. Running security features on many VDOMs at once can limit resources available for basic processing. If you require many VDOMs, all with active security features, it is recommended to upgrade to a more powerful FortiGate unit.

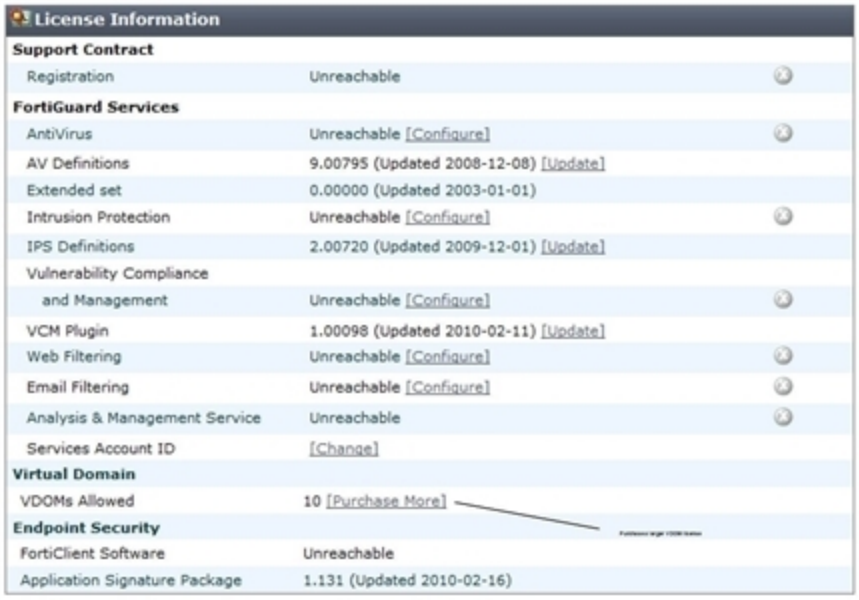
It is important to backup your configuration before upgrading the VDOM license on your FortiGate unit or units, especially with FortiGate units in HA mode.

To obtain a VDOM license key

1. Log in with a super_admin account.
2. Go to **System > Dashboard > Status**.
3. Record your FortiGate unit serial number as shown in System Information.
4. Under **License Information > Virtual Domain**, select **Purchase More**.

If you do not see the **Purchase More** option on the System Dashboard, your FortiGate model does not support more than 10 VDOMs.

VDOM License Information



5. You will be taken to the Fortinet customer support website where you can log in and purchase a license key for 25, 50, 100, 250, 500, or more VDOMs.
6. When you receive your license key, go to the Dashboard and select **Upload License** under **License Information**, **Virtual Domains**.
7. In the **Input License Key** field, enter the 32-character license key you received from Fortinet customer support.
8. Select **Apply**.

To verify the new VDOM license, in global configuration go to **System > Dashboard**. Under **License Information**, **Virtual Domains** the maximum number of VDOMs allowed is shown.

VDOMs created on a registered FortiGate unit are recognized as real devices by any connected FortiAnalyzer unit. The FortiAnalyzer unit includes VDOMs in its total number of registered devices. For example, if three FortiGate units are registered on the FortiAnalyzer unit and they contain a total of four VDOMs, the total number of registered FortiGate units on the FortiAnalyzer unit is seven. For more information, see the FortiAnalyzer Administration Guide.

Logging in to VDOMs

Only super_admin administrator accounts can access all global settings on the FortiGate unit and all of the VDOMs as well. Other administrator accounts can access and configure only their single VDOM and they must connect to an interface that is part of that VDOM. For example, administratorB is the admin for vdomB. If he tries to log into vdomA, or an interface that is part of vdomA he will not be able to log on. For more information on administrators in VDOMs, see Administrators in Virtual Domains.

Management services communicate using the management VDOM, which is the root VDOM by default. For more information, see Changing the management virtual domain.

Management traffic requires an interface that has access to the Internet. If there is no interface assigned to the VDOM containing the management traffic, services including updates will not function. For more information, see Changing the management virtual domain.

To access a VDOM with a super_admin account - web-based manager:

1. Log in with a super_admin account.
2. In the **Virtual Domains** menu on the left-hand side, select the VDOM to configure.
   The menu will expand to show the various pages and settings for that VDOM.
3. When you have finished configuring the VDOM, you can
   - open the **Global** menu to return to global configuration
   - log out

To access a VDOM with a super_admin account - CLI:

With the super_admin, logging into the CLI involves also logging into the specific VDOM. If you need a reminder, use `edit ?` to see a list of existing VDOMs before you editing a VDOM.

If you misspell a VDOM you are trying to switch to, you will create a new VDOM by that name. Any changes you make will be part of the new VDOM, and not the intended VDOM. If you are having problems where your changes aren't visible, back up to the top level and use `edit ?` to see a list of VDOMs to ensure this has not happened. If it has happened, see Deleting a VDOM.

```
config vdom
   edit ?
   edit <chosen_vdom>
      ..
      <enter vdom related commands>
      ..
   end
exit
```

To access a VDOM with a non super_admin account - web-based manager:

1. Connect to the FortiGate unit using an interface that belongs to the VDOM to be configured.
2. Log in using an administrator account that has access to the VDOM.
   The main web-based manager page opens. The interface is largely the same as if the device has VDOMs disabled. From here you can access VDOM-specific settings.

To access a VDOM with a non-super_admin account - CLI:

A non-super_admin account has access to only one VDOM and must log in through an interface that belongs to the same VDOM, but the process is the same as logging into a non-VDOM unit.

```
Login: regular_admin
Password: <password>
..
<enter vdom related commands>
..
exit
```

Configuring Virtual Domains

Only a super_admin administrator account such as the default “admin” account can create, disable, or delete VDOMs. That account can create additional administrators for each VDOM.

This section includes:

- Creating a Virtual Domain
- Disabling a Virtual Domain
- Deleting a VDOM
- Administrators in Virtual Domains

Creating a Virtual Domain

Once you have enabled Virtual Domains on your FortiGate unit, you can create additional Virtual Domains beyond the default root Virtual Domain.

By default new Virtual Domains are set to NAT/Route operation mode. If you want a Virtual Domain to be in Transparent operation mode, you must manually change it. See Virtual Domains in Transparent mode.

You can name new Virtual Domains as you like with the following restrictions:

- only letters, numbers, “-”, and “_” are allowed
- no more than 11 characters are allowed
- no spaces are allowed
- VDOMs cannot have the same names as interfaces, zones, switch interfaces, or other VDOMs.

When creating large numbers of VDOMs you should not enable advanced features such as proxies, web filtering, and antivirus due to limited FortiGate unit resources. Also when creating large numbers of VDOMs, you may experience reduced performance for the same reason.

To create a VDOM - web-based manager:

1. Log in with a super_admin account.
2. Go to **System > Dashboard > Status** and ensure that Virtual Domains are enabled. If not, see Enabling and accessing Virtual Domains.
3. Select **System > VDOM > VDOM**.
4. Select **Create New**.
5. Enter a unique name for your new VDOM.
6. Enter a short and descriptive comment to identify this VDOM.
7. Select **OK**.

Repeat Steps4 through 7 to add additional VDOMs.

To create a VDOM - CLI:

```
config vdom
   edit <new_vdom_name>
end
```

If you want to edit an existing Virtual Domain in the CLI, and mistype the name a new Virtual Domain will be created with this new misspelled name. If you notice expected configuration changes are not visible, this may be the reason. You should periodically check your VDOM list to ensure there are none of these misspelled VDOMs present.

Disabling a Virtual Domain

The status of a VDOM can be Enabled, or Disabled.

Active status VDOMs can be configured. Active is the default status when a VDOM is created. The management VDOM must be an Active VDOM. For more information on the management VDOM, see Changing the management virtual domain.

Disabled status VDOMs are considered “offline”. The configuration remains, but you cannot use the VDOM, and only the super_admin administrator can view it. You cannot delete a disabled VDOM without first enabling it, and removing references to it like usual—there is no **Delete** icon for disabled status VDOMs. You can assign interfaces to a disabled VDOM. See Deleting a VDOM.

The following procedures show how to disable a VDOM called “test-vdom”.

To disable a VDOM - web-based manager:

1. Go to **Global > VDOM** > **VDOM**.
2. Open the VDOM for editing.
3. Ensure **Enable** is not selected and then select **OK**.
   The VDOM’s Enable icon in the VDOM list is a grey X.

To disable a VDOM - CLI:

```
config vdom
   edit test-vdom
      config system settings
         set status disable
      end
end
```

To enable a VDOM - web-based manager:

1. Go to **Global > VDOM** > **VDOM**.
2. Open the VDOM for editing.
3. Ensure **Enable** is selected and then select **OK**.
   The VDOM’s Enable icon in the VDOM list is a green checkmark.

To enable a VDOM - CLI:

```
config vdom
   edit test-vdom
      config system settings
         set status enable
      end
end
```

Deleting a VDOM

Deleting a VDOM removes it from the FortiGate unit configuration.

Before you can delete a VDOM, all references to it must be removed. This includes any objects listed in Per-VDOM settings - web-based manager. If there are any references to the VDOM remaining, you will see an error message and not be able to delete the VDOM.

The VDOM must also be enabled. A disabled VDOM cannot be deleted. You cannot delete the root VDOM or the management VDOM.

Before deleting a VDOM, a good practice is to reset any interface referencing that VDOM to its default configuration, with “root” selected as the Virtual Domain.

The following procedures show how to delete the `test-vdom` VDOM.

To delete a VDOM - web-based manager:

1. Go to **Global > VDOM > VDOM**.
2. Select the check box for the VDOM and then select the **Delete** icon.

   If the **Delete** icon is not active, there are still references to the VDOM that must first be removed. The **Delete** icon is available when all the references to this VDOM are removed.
3. Confirm the deletion.

To delete a VDOM - CLI:

```
config vdom
   delete test-vdom
end
```

Removing references to a VDOM

When you are going to delete a VDOM, all references to that VDOM must first be removed. It can be difficult to find all the references to the VDOM. This section provides a list of common objects that must be removed before a VDOM can be deleted, and a CLI command to help list the dependencies.

Interfaces are an important part of VDOMs. If you can move all the interfaces out of a VDOM, generally you will be able to delete that VDOM.

Common objects that refer to VDOMs

When you are getting ready to delete a VDOM check for, and remove the following objects that refer to that VDOM or its components:

- Routing - both static and dynamic routes
- Firewall addresses, policies, groups, or other settings
- Security Features/Profiles
- VPN configuration
- Users or user groups

- Logging
- DHCP servers
- Network interfaces, zones, custom DNS servers
- VDOM Administrators

Administrators in Virtual Domains

When Virtual Domains are enabled, permissions change for administrators. Administrators are now divided into per-VDOM administrators, and `super_admin` administrators. Only `super_admin` administrator accounts can create other administrator accounts and assign them to a VDOM.

This section includes:

- Administrator VDOM permissions
- Creating administrators for Virtual Domains
- Virtual Domain administrator dashboard display

Administrator VDOM permissions

Different types of administrator accounts have different permissions within VDOMs. For example, if you are using a super_admin profile account, you can perform all tasks. However, if you are using a regular admin account, the tasks available to you depend on whether you have read only or read/write permissions. The following table shows what tasks can be performed by which administrators.

Table 3: Administrator VDOM permissions

Tasks	Regular administrator account		Super_admin profile administrator account
	Read only permission	Read/write permission	
View global settings	yes	yes	yes
Configure global settings	no	no	yes
Create or delete VDOMs	no	no	yes
Configure multiple VDOMs	no	no	yes
Assign interfaces to a VDOM	no	no	yes
Revision Control Backup and Restore	no	no	yes
Create VLANs	no	yes - for 1 VDOM	yes - for all VDOMs
Assign an administrator to a VDOM	no	no	yes
Create additional admin accounts	no	yes - for 1 VDOM	yes - for all VDOMs
Create and edit protection profiles	no	yes - for 1 VDOM	yes - for all VDOMs

The only difference in admin accounts when VDOMs are enabled is selecting which VDOM the admin account belongs to. Otherwise, by default the administration accounts are the same as when VDOMs are disabled and closely resemble the `super_admin` account in their privileges.

Creating administrators for Virtual Domains

Using the admin administrator account, you can create additional administrator accounts and assign them to VDOMs.

The newly-created administrator can access the FortiGate unit only through network interfaces that belong to their assigned VDOM or through the console interface. The network interface must be configured to allow management access, such as HTTPS and SSH. Without these in place, the new administrator will not be able to access the FortiGate unit and will have to contact the super_admin administrator for access.

The following procedure creates a new Local administrator account called `admin_sales` with a password of `fortinet` in the `sales` VDOM using the `admin_prof` default profile.

To create an administrator for a VDOM - web-based manager:

1. Log in with a super_admin account.
2. Go to **System > Admin > Administrators**.
3. Select **Create New**.
4. Select **Regular** for Type, as you are creating a Local administrator account.
5. Enter the necessary information about the administrator: email, password, etc.
6. If this admin will be accessing the VDOM from a particular IP address or subnet, enable **Restrict this Admin Login from Trusted Hosts Only** and enter the IP in **Trusted Host #1**. See Using trusted hosts.
7. Select `prof_admin` for the **Admin Profile**.
8. Select `sales` from the list of **Virtual Domains**.
9. Select **OK**.

To create administrators for VDOMs - CLI:

```
config global
   config system admin
      edit <new_admin_name>
         set vdom <vdom_for_this_account>
         set password <pwd>
         set accprofile <an_admin_profile>
         ...
      end
```

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiGate unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the web-based manager and to the CLI when accessed through Telnet or SSH. CLI access through the console is not affected.

The trusted host addresses all default to 0.0.0.0/0.0.0.0 for IPv4, or ::/0 for IPv6. If you set one of the zero addresses to a non-zero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0 or ::0. However, this configuration is less secure.

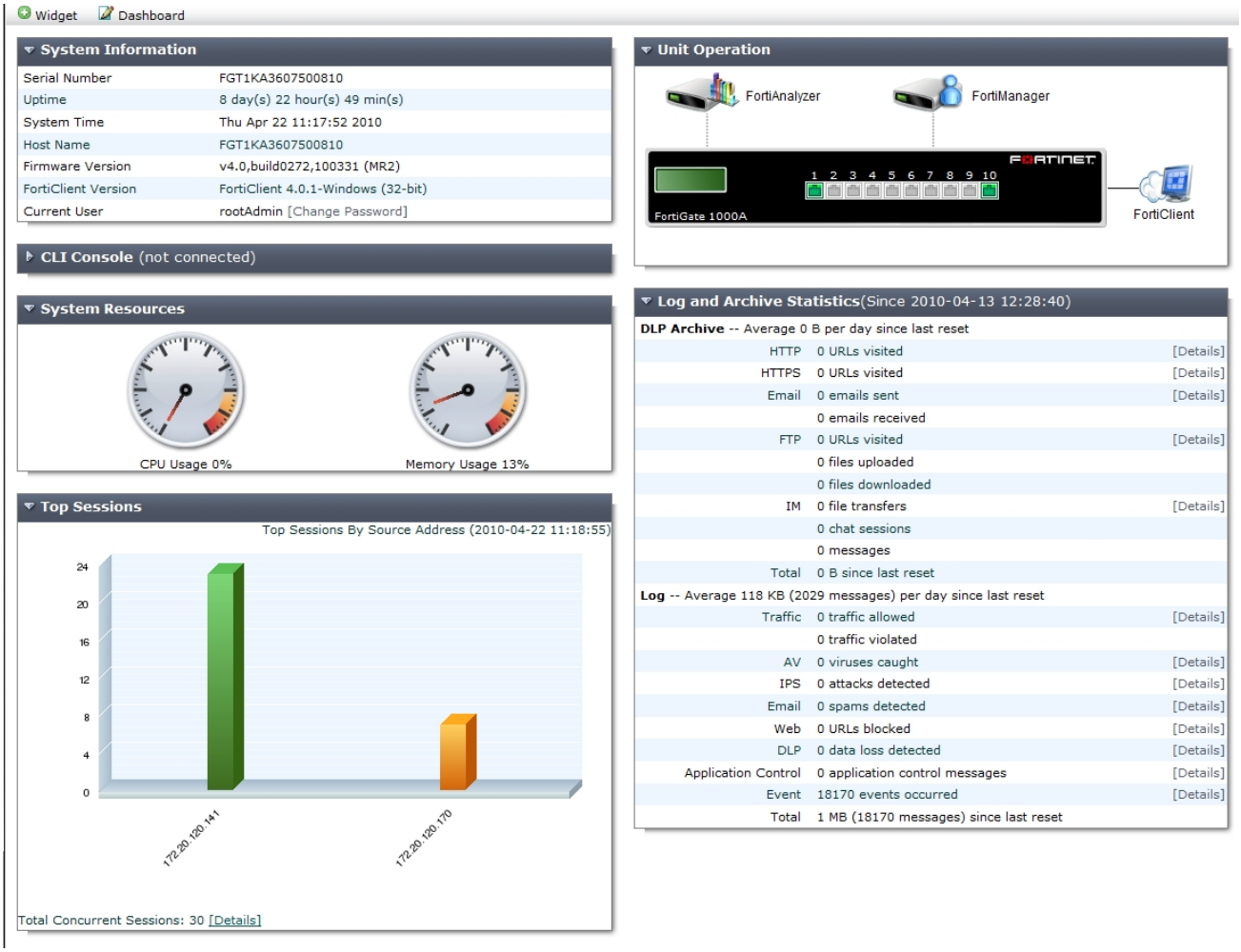
Virtual Domain administrator dashboard display

When administrators logs into their virtual domain, they see a different dashboard than the global administrator will see. The VDOM dashboard displays information only relevant to that VDOM — no global or other VDOM information is displayed.

Table 4: VDOM dashboard information

Information	per-VDOM	Global
System Information	read-only	yes
License Information	no	yes
CLI console	yes	yes
Unit Operation	read-only	yes
Alert Message Console	no	yes
Top Sessions	limited to VDOM sessions	yes
Traffic	limited to VDOM interfaces	yes
Statistics	yes	yes

VDOM administrator dashboard



Virtual Domains in NAT/Route mode

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that each function as independent units. Each virtual domain has separate routing and security policies. A single FortiGate unit with virtual domains is flexible enough to serve multiple departments of an organization, separate organizations, or be the basis for a service provider's managed security service.

The examples in this chapter are intended to be followed in order as procedures build on previous procedures. If you do not complete the previous procedures, the procedure you are working on may not work properly. If this happens, consult previous procedures or FortiGate documentation.

This chapter contains the following sections:

- Virtual domains in NAT/Route mode
- Example NAT/Route VDOM configuration
- Figure 9: Example VDOM configuration

Virtual domains in NAT/Route mode

Once you have enabled virtual domains and created one or more VDOMs, you need to configure them. Configuring VDOMs on your FortiGate unit includes tasks such as the ones listed here; while you may not require all for your network topology, it is recommended that you perform them in the order given:

- Changing the management virtual domain
- Configuring interfaces in a NAT/Route VDOM
- Configuring VDOM routing
- Configuring security policies for NAT/Route VDOMs
- Configuring security profiles for NAT/Route VDOMs

Changing the management virtual domain

The management virtual domain is the virtual domain where all the management traffic for the FortiGate unit originates. This management traffic needs access to remote servers, such as FortiGuard services and NTP, to perform its duties. It needs access to the Internet to send and receive this traffic.

Management traffic includes, but is not limited to

- DNS lookups
- logging to FortiAnalyzer or syslog
- FortiGuard service
- sending alert emails
- Network time protocol traffic (NTP)
- Sending SNMP traps
- Quarantining suspicious files and email.

By default the management VDOM is the root domain. When other VDOMs are configured on your FortiGate unit, management traffic can be moved to one of these other VDOMs.

Reasons to move the management VDOM include selecting a non-root VDOM to be your administration VDOM, or the root VDOM not having an interface with a connection to the Internet.

You cannot change the management VDOM if any administrators are using RADIUS authentication.

The following procedure will change the management VDOM from the default `root` to a VDOM named `mgmt_vdom`. It is assumed that `mgmt_vdom` has already been created and has an interface that can access the Internet.

To change the management VDOM - web-based manager:

1. Select **Global > VDOM > VDOM.**
2. Select the checkbox next to the required VDOM.
3. Select **Switch Management.**
   The current management VDOM is shown in square brackets, “[root]” for example.

To change the management VDOM - CLI:

```
config global
   config system global
      set management-vdom mgmt_vdom
   end
```

Management traffic will now originate from `mgmt_vdom`.

Configuring interfaces in a NAT/Route VDOM

A VDOM must contain at least two interfaces to be useful. These can be physical interfaces or VLAN interfaces. By default, all physical interfaces are in the root VDOM. When you create a new VLAN, it is in the root VDOM by default.

When there are VDOMs on the FortiGate unit in both NAT and Transparent operation modes, some interface fields will be displayed as “-” on **System > Network > Interfaces**. Only someone with a super_admin account can view all the VDOMs.

When moving an interface to a different VDOM, firewall IP pools and virtual IPs for this interface are deleted. You should manually delete any routes that refer to this interface. Once the interface has been moved to the new VDOM, you can add these services to the interface again.

When configuring VDOMs on FortiGate units with accelerated interfaces you must assign both interfaces in the pair to the same VDOM for those interfaces to retain their acceleration. Otherwise they will become normal interfaces.

This section includes the following topics:

- Adding a VLAN to a NAT/Route VDOM
- Moving an interface to a VDOM
- Deleting an interface
- Adding a zone to a VDOM

Adding a VLAN to a NAT/Route VDOM

The following example shows one way that multiple companies can maintain their security when they are using one FortiGate unit with VLANs that share interfaces on the unit.

This procedure will add a VLAN interface called `client1-v100` with a VLAN ID of 100 to an existing VDOM called `client1` using the physical interface called `port2`.

The physical interface does not need to belong to the VDOM that the VLAN belongs to.

To add a VLAN subinterface to a VDOM - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	client1-v100
Interface	port2
VLAN ID	100
Virtual Domain	Client1
Addressing mode	Manual
IP/Netmask	172.20.120.110/255.255.255.0
Administrative Access	HTTPS, SSH

You will see an expand arrow added to the port2 interface. When the arrow is expanded, the interface shows the `client1-v100` VLAN subinterface.

To add a VLAN subinterface to a VDOM - CLI:

```
config global
   config system interface
      edit client1-v100
         set type vlan
         set vlanid 100
         set vdom Client1
         set interface port2
         set ip 172.20.120.110 255.255.255.0
         set allowaccess https ssh
      end
```

Moving an interface to a VDOM

Interfaces belong to the root VDOM by default. Moving an interface is the same procedure no matter if its moving from the root VDOM or a any other VDOM.

If you have an accelerated pair of physical interfaces both interfaces must be in the same VDOM or you will lose their acceleration.

The following procedure will move the port3 interface to the Client2 VDOM. This is a common action when configuring a VDOM. It is assumed that the Client2 VDOM has already been created. It is also assumed that your FortiGate unit has a port3 interface. If you are using a different model, your physical interfaces may not be named `port2`, `external` or `port3`.

To move an existing interface to a different VDOM - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** for the port3 interface.
3. Select `Client2` as the new **Virtual Domain**.
4. Select **OK**.

To move an existing interface to a different VDOM - CLI:

```
config global
   config system interface
      edit port3
         set vdom Client2
      end
```

Deleting an interface

Before you can delete a virtual interface, or move an interface from one VDOM to another, all references to that interface must be removed. For a list of objects that can refer to an interface see Per-VDOM settings - web-based manager.

The easiest way to be sure an interface can be deleted is when the Delete icon is no longer greyed out. If it remains greyed out when an interface is selected, that interface still has objects referring to it, or it is a physical interface that cannot be deleted.

To delete a virtual interface - web-based manager:

1. Ensure all objects referring to this interface have been removed.
2. Select **Global > Network > Interfaces**.
3. Select the interface to delete.
4. Select the delete icon.

Adding a zone to a VDOM

Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation. You can configure policies for connections to and from a zone, but not between interfaces in a zone.

Zones are VDOM-specific. A zone cannot be moved to a different VDOM. Any interfaces in a zone cannot be used in another zone. To move a zone to a new VDOM requires deleting the current zone and re-creating a zone in the new VDOM.

The following procedure will create a zone called `accounting` in the `client2` VDOM. It will not allow intra-zone traffic, and both `port3` and `port2` interfaces belong to this zone. This is a method of grouping and isolating traffic over particular interfaces—it is useful for added security and control within a larger network.

To add a zone to a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **System > Network > Interfaces**.
3. Select **Create New > Zone**.
4. Enter the following information and select **OK**:

Zone Name	accounting
Block intra-zone traffic	Select
Interface Members	port3, port2

To add a zone to a VDOM - CLI:

```
config vdom
   edit client2
      config system zone
         edit accounting
            set interface port3 port2
            set intrazone deny
         end
   end
```

Configuring VDOM routing

Routing is VDOM-specific. Each VDOM should have a default static route configured as a minimum. Within a VDOM, routing is the same as routing on your FortiGate unit without VDOMs enabled.

When configuring dynamic routing on a VDOM, other VDOMs on the FortiGate unit can be neighbors. The following topics give a brief introduction to the routing protocols, and show specific examples of how to configure dynamic routing for VDOMs. Figures are included to show the FortiGate unit configuration after the successful completion of the routing example.

This section includes:

- Default static route for a VDOM
- Dynamic Routing in VDOMs

Default static route for a VDOM

The routing you define applies only to network traffic entering non-ssl interfaces belonging to this VDOM. Set the administrative distance high enough, typically 20, so that automatically configured routes will be preferred to the default.

In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure will create a default static route for this VDOM. The route has a destination IP of 0.0.0.0, on the port3 interface. It has a gateway of 10.10.10.1, and an administrative distance of 20.

The values used in this procedure are very standard, and this procedure should be part of configuring all VDOMs.

To add a default static route for a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Router > Static > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2
Gateway	10.10.10.1
Distance	20

To add a default static route for a VDOM - CLI:

```
config vdom
   edit client2
      config router static
         edit 4
            set device port2
            set dst 0.0.0.0 0.0.0.0
            set gateway 10.10.10.1
            set distance 20
         end
   end
```

Dynamic Routing in VDOMs

Dynamic routing is VDOM-specific, like all other routing. Dynamic routing configuration is the same with VDOMs as with your FortiGate unit without VDOMs enabled, once you are at the routing menu. If you have multiple VDOMs configured, the dynamic routing configuration between them can become quite complex.

VDOMs provide some interesting changes to dynamic routing. Each VDOM can be a neighbor to the other VDOMs. This is useful in simulating a dynamic routing area or AS or network using only your FortiGate unit.

You can separate different types of routing to different VDOMs if required. This allows for easier troubleshooting. This is very useful if your FortiGate unit is on the border of a number of different routing domains.

For more information on dynamic routing in FortiOS, see Dynamic Routing OverviewDynamic Routing Overview.

Inter-VDOM links must have IP addresses assigned to them if they are part of a dynamic routing configuration. Inter-VDOM links may or may not have IP addresses assigned to them. Without IP addresses, you need to be careful how you configure routing. While the default static route can be assigned an address of 0.0.0.0 and rely instead on the interface, dynamic routing almost always requires an IP address.

RIP

The RIP dynamic routing protocol uses hop count to determine the best route, with a hop count of 1 being directly attached to the interface and a hop count of 16 being unreachable. For example if two VDOMs on the same FortiGate unit are RIP neighbors, they have a hop count of 1.

OSPF

OSPF communicates the status of its network links to adjacent neighbor routers instead of the complete routing table. When compared to RIP, OSPF is more suitable for large networks, it is not limited by hop count, and is more complex to configure. For smaller OSPF configurations its easiest to just use the backbone area, instead of multiple areas.

BGP

BGP is an Internet gateway protocol (IGP) used to connect autonomous systems (ASes) and is used by Internet service providers (ISPs). BGP stores the full path, or path vector, to a destination and its attributes which aid in proper routing.

Configuring security policies for NAT/Route VDOMs

Security policies are VDOM-specific. This means that all firewall settings for a VDOM, such as firewall addresses and security policies, are configured within the VDOM.

In VDOMs, all firewall related objects are configured per-VDOM including addresses, service groups, security profiles, schedules, traffic shaping, and so on. If you want firewall addresses, you will have to create them on each VDOM separately. If you have many addresses, and VDOMs this can be tedious and time consuming. Consider using a FortiManager unit to manage your VDOM configuration — it can get firewall objects from a configured VDOM or FortiGate unit, and push those objects to many other VDOMs or FortiGate units. See the FortiManager Administration Guide.

You can customize the **Policy** display by including some or all columns, and customize the column order onscreen. Due to this feature, security policy screenshots may not appear the same as on your screen.

Configuring a security policy for a VDOM

Your security policies can involve only the interfaces, zones, and firewall addresses that are part of the current VDOM, and they are only visible when you are viewing the current VDOM. The security policies of this VDOM filter the network traffic on the interfaces and VLAN subinterfaces in this VDOM.

A firewall service group can be configured to group multiple services into one service group. When a descriptive name is used, service groups make it easier for an administrator to quickly determine what services are allowed by a security policy.

In the following procedure, it is assumed that a VDOM called `Client2` exists. The procedure will configure an outgoing security policy. The security policy will allow all HTTPS and SSH traffic for the `SalesLocal` address group on VLAN_200 going to all addresses on port3. This traffic will be scanned and logged.

To configure a security policy for a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Policy > Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_200
Source Address	SalesLocal
Destination Interface/Zone	port3
Destination Address	any
Schedule	always
Service	Multiple - HTTPS, SSH
Action	ACCEPT
Log Allowed Traffic	enable

To configure a security policy for a VDOM - CLI:

```
config vdom
   edit Client2
      config firewall policy
         edit 12
            set srcintf VLAN_200
            set srcaddr SalesLocal
            set dstintf port3(dmz)
            set dstaddr any
            set schedule always
            set service HTTPS SSH
            set action accept
            set status enable
            set logtraffic enable
         end
   end
```

Configuring security profiles for NAT/Route VDOMs

In NAT/Route VDOMs, security profiles are exactly like regular FortiGate unit operation with one exception. In VDOMs, there are no default security profiles.

If you want security profiles in VDOMs, you must create them yourself. If you have many security profiles to create in each VDOM, you should consider using a FortiManager unit. It can get existing profiles from a VDOM or FortiGate unit, and push those profiles down to multiple other VDOMs or FortiGate units. See the FortiManager Administration Guide.

When VDOMs are enabled, you only need one FortiGuard license for the physical unit, and download FortiGuard updates once for the physical unit. This can result in a large time and money savings over multiple physical units if you have many VDOMs.

Configuring VPNs for a VDOM

Virtual Private Networking (VPN) settings are VDOM-specific, and must be configured within each VDOM. Configurations for IPsec Tunnel, IPsec Interface, PPTP and SSL are VDOM-specific. However, certificates are shared by all VDOMs and are added and configured globally to the FortiGate unit.

Example NAT/Route VDOM configuration

Company A and Company B each have their own internal networks and their own ISPs. They share a FortiGate unit that is configured with two separate VDOMs, with each VDOM running in NAT/Route mode enabling separate configuration of network protection profiles. Each ISP is connected to a different interface on the FortiGate unit.

This network example was chosen to illustrate one of the most typical VDOM configurations.

This example has the following sections:

- Network topology and assumptions
- General configuration steps
- Creating the VDOMs
- Configuring the FortiGate interfaces
- Configuring the vdomA VDOM
- Configuring the vdomB VDOM
- Testing the configuration

Network topology and assumptions

Both companies have their own ISPs and their own internal interface, external interface, and VDOM on the FortiGate unit.

For easier configuration, the following IP addressing is used:

- all IP addresses on the FortiGate unit end in ".2" such as 10.11.101.2.
- all IP addresses for ISPs end in ".7", such as 172.20.201.7.
- all internal networks are 10.*.*.* networks, and sample internal addresses end in ".55".

The IP address matrix for this example is as follows.

Address	Company A	Company B
ISP	172.20.201.7	192.168.201.7
Internal network	10.11.101.0	10.12.101.0
FortiGate / VDOM	172.20.101.2 (port1) 10.11.101.2 (port4)	192.168.201.2 (port3) 10.12.101.2 (port2)

The Company A internal network is on the 10.11.101.0/255.255.255.0 subnet. The Company B internal network is on the 10.12.101.0/255.255.255.0 subnet.

There are no switches or routers required for this configuration.

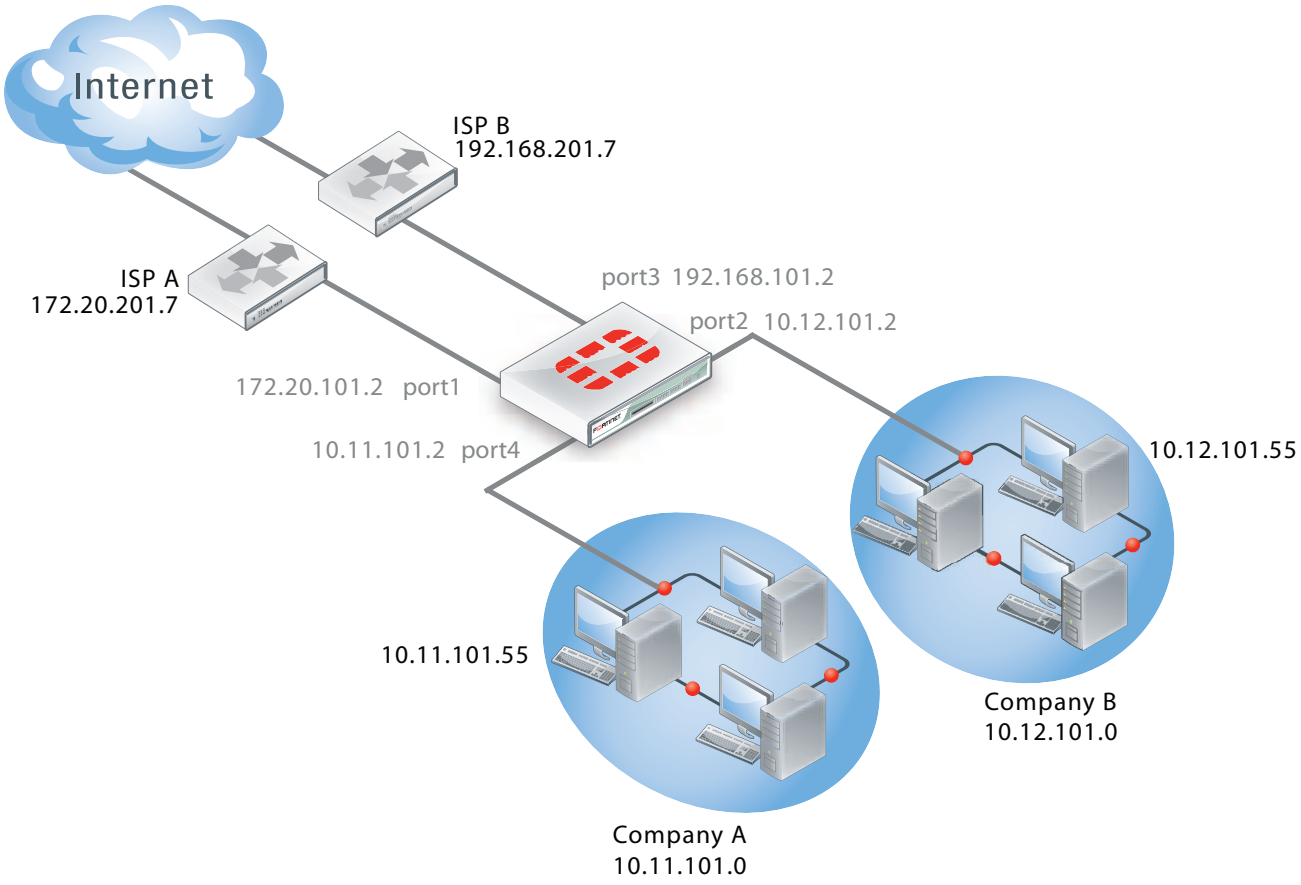
There are no VLANs in this network topology.

The interfaces used in this example are port1 through port4. Different FortiGate models may have different interface labels. port1 and port3 are used as external interfaces. port2 and port4 are internal interfaces.

The administrator is a super_admin account. If you are a using a non-super_admin account, refer to "Global and per-VDOM settings" to see which parts a non-super_admin account can also configure.

When configuring security policies in the CLI always choose a policy number that is higher than any existing policy numbers, select `services` before `profile-status`, and `profile-status` before `profile`. If these commands are not entered in that order, they may not be available to enter.

Figure 9: Example VDOM configuration



General configuration steps

For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the FortiGate interfaces
3. Configuring the vdomA VDOM, and Configuring the vdomB VDOM
4. Testing the configuration

Creating the VDOMs

In this example, two new VDOMs are created — vdomA for Company A and vdomB for Company B. These VDOMs will keep the traffic for these two companies separate while enabling each company to access its own ISP.

To create two VDOMs - web-based manager:

1. Log in with a super_admin account.
2. Go to **Global > VDOM > VDOM**, and select **Create New**.
3. Enter `vdomA` and select **OK**.
4. Select **OK** again to return to the VDOM list.
5. Select **Create New**.
6. Enter `vdomB` and select **OK**.

To create two VDOMs - CLI:

```
config vdom
   edit vdomA
   next
   edit vdomB
end
```

Configuring the FortiGate interfaces

This section configures the interfaces that connect to the companies' internal networks, and to the companies' ISPs.

All interfaces on the FortiGate unit will be configured with an IP address ending in ".2" such as 10.11.101.2. This will simplify network administration both for the companies, and for the FortiGate unit global administrator. Also the internal addresses for each company differ in the second octet of their IP address - Company A is 10.11.*, and Company B is 10.12.*.

This section includes the following topics:

- Configuring the vdomA interfaces
- Configuring the vdomB interfaces

If you cannot change the VDOM of an network interface it is because something is referring to that interface that needs to be deleted. Once all the references are deleted the interface will be available to switch to a different VDOM. For example a common reference to the external interface is the default static route entry. See Configuring interfaces in a NAT/Route VDOM.

Configuring the vdomA interfaces

The `vdomA` VDOM includes two FortiGate unit interfaces: port1 and external.

The port4 interface connects the Company A internal network to the FortiGate unit, and shares the internal network subnet of 10.11.101.0/255.255.255.0.

The external interface connects the FortiGate unit to ISP A and the Internet. It shares the ISP A subnet of 172.20.201.0/255.255.255.0.

To configure the vdomA interfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port1 interface.
3. Enter the following information and select **OK**:

Virtual Domain	vdomA
Addressing mode	Manual
IP/Netmask	172.20.101.2/255.255.255.0

4. Select **Edit** on the port4 interface.
5. Enter the following information and select **OK**:

Virtual Domain	vdomA
Addressing mode	Manual
IP/Netmask	10.11.101.2/255.255.255.0

To configure the vdomA interfaces - CLI:

```
config global
   config system interface
      edit port1
         set vdom vdomA
         set mode static
         set ip 172.20.101.2 255.255.255.0
      next
      edit port4
         set vdom vdomA
         set mode static
         set ip 10.11.101.2 255.255.255.0
      end
```

Configuring the vdomB interfaces

The `vdomB` VDOM uses two FortiGate unit interfaces: port2 and port3.

The port2 interface connects the Company B internal network to the FortiGate unit, and shares the internal network subnet of 10.12.101.0/255.255.255.0.

The port3 interface connects the FortiGate unit to ISP B and the Internet. It shares the ISP B subnet of 192.168.201.0/255.255.255.0.

To configure the vdomB interfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port3 interface.

3. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	192.168.201.2/255.255.255.0

4. Select **Edit** on the port2 interface.
5. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	10.12.101.2/255.255.255.0

To configure the vdomB interfaces - CLI:

```
config global
   config system interface
      edit port3
         set vdom vdomB
         set mode static
         set ip 192.168.201.2 255.255.255.0
      next
      edit port2
         set vdom vdomB
         set mode static
         set ip 10.12.101.2 255.255.255.0
   end
```

Configuring the vdomA VDOM

With the VDOMs created and the ISPs connected, the next step is to configure the vdomA VDOM.

Configuring the vdomA includes the following:

- Adding vdomA firewall addresses
- Adding the vdomA security policy
- Adding the vdomA default route

Adding vdomA firewall addresses

You need to define the addresses used by Company A's internal network for use in security policies. This internal network is the 10.11.101.0/255.255.255.0 subnet.

The FortiGate unit provides one default address, "all", that you can use when a security policy applies to all addresses as the source or destination of a packet.

To add the vdomA firewall addresses - web-based manager:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Firewall Objects > Address > Address**.

3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Ainternal
Type	Subnet / IP Range
Subnet / IP Range	10.11.101.0/255.255.255.0
Interface	port4

To add the vdomA VDOM firewall addresses - CLI:

```
config vdom
   edit vdomA
      config firewall address
         edit Ainternal
            set type ipmask
            set subnet 10.11.101.0 255.255.255.0
      end
   end
```

Adding the vdomA security policy

You need to add the `vdomA` security policy to allow traffic from the internal network to reach the external network, and from the external network to internal as well. You need two policies for this domain.

To add the vdomA security policy - web-based manager:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Policy > Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Source Interface/Zone	port4
Source Address	Ainternal
Destination Interface/Zone	port1
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

5. Select **Create New**.
6. Enter the following information and select **OK**:

Source Interface/Zone	port1
Source Address	all
Destination Interface/Zone	port4
Destination Address	Ainternal
Schedule	Always
Service	ANY
Action	ACCEPT

To add the vdomA security policy - CLI:

```
config vdom
   edit vdomA
      config firewall policy
         edit 1
            set srcintf port4
            set srcaddr Ainternal
            set dstintf port1
            set dstaddr all
            set schedule always
            set service ANY
            set action accept
            set status enable
         next
         edit 2
            set srcintf port1
            set srcaddr all
            set dstintf port4
            set dstaddr Ainternal
            set schedule always
            set service ANY
            set action accept
            set status enable
         end
```

Adding the vdomA default route

You also need to define a default route to direct packets from the Company A internal network to ISP A. Every VDOM needs a default static route, as a minimum, to handle traffic addressed to external networks such as the Internet.

The administrative distance should be set slightly higher than other routes. Lower admin distances will get checked first, and this default route will only be used as a last resort.

To add a default route to the vdomA - web-based manager:

1. For **Virtual Domains**, select **vdomA**
2. Go to **Router > Static > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port1
Gateway	172.20.201.7
Distance	20

To add a default route to the vdomA - CLI:

```
config vdom
   edit vdomA
      config router static
         edit 1
            set device port1
            set gateway 172.20.201.7
         end
```

Configuring the vdomB VDOM

In this example, the vdomB VDOM is used for Company B. Firewall and routing settings are specific to a single VDOM.

vdomB includes the FortiGate port2 interface to connect to the Company B internal network, and the FortiGate port3 interface to connect to ISP B. Security policies are needed to allow traffic from port2 to external and from external to port2 interfaces.

This section includes the following topics:

- Adding the vdomB firewall address
- Adding the vdomB security policy
- Adding a default route to the vdomB VDOM

Adding the vdomB firewall address

You need to define addresses for use in security policies. In this example, the vdomB VDOM needs an address for the port2 interface and the “all” address.

To add the vdomB firewall address - web-based manager:

1. In **Virtual Domains**, select **vdomB**.
2. Go to **Firewall Objects > Address > Address**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Binternal
Type	Subnet / IP Range
Subnet / IP Range	10.12.101.0/255.255.255.0
Interface	port2

To add the vdomB firewall address - CLI:

```
config vdom
   edit vdomB
      config firewall address
         edit Binternal
            set type ipmask
            set subnet 10.12.101.0 255.255.255.0
         end
   end
```

Adding the vdomB security policy

You also need a security policy for the Company B domain. In this example, the security policy allows all traffic.

To add the vdomB security policy - web-based manager:

1. Log in with a super_admin account.
2. In **Virtual Domains**, select vdomB.
3. Go to **Policy > Policy**.
4. Select **Create New**.
5. Enter the following information and select **OK**:

Source Interface/Zone	port2
Source Address	Binternal
Destination Interface/Zone	port3
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

6. Select **Create New**.
7. Enter the following information and select **OK**:

Source Interface/Zone	port3
Source Address	all
Destination Interface/Zone	port2
Destination Address	Binternal
Schedule	Always
Service	ANY
Action	ACCEPT

To add the vdomB security policy - CLI:

```
config vdom
   edit vdomB
      config firewall policy
         edit 1
            set srcintf port2
            set dstintf port3
            set srcaddr Binternal
            set dstaddr all
            set schedule always
            set service ANY
            set action accept
            set status enable
         edit 1
            set srcintf port3
            set dstintf port2
            set srcaddr all
            set dstaddr Binternal
            set schedule always
            set service ANY
            set action accept
            set status enable
         end
   end
```

Adding a default route to the vdomB VDOM

You need to define a default route to direct packets to ISP B.

To add a default route to the vdomB VDOM - web-based manager:

1. Log in as the super_admin administrator.
2. In **Virtual Domains**, select vdomB.
3. Go to **Router > Static > Static Routes**.
4. Select **Create New**.
5. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3
Gateway	192.168.201.7
Distance	20

To add a default route to the vdomB VDOM - CLI:

```
config vdom
   edit vdomB
      config router static
         edit 1
            set dst 0.0.0.0/0
```

```
            set device external
            set gateway 192.168.201.7
        end
    end
```

Testing the configuration

Once you have completed configuration for both company VDOMs, you can use diagnostic commands, such as `tracert` in Windows, to test traffic routed through the FortiGate unit. Alternately, you can use the `traceroute` command on a Linux system with similar output.

Possible errors during the traceroute test are:

- "`* * * Request timed out`" - the trace was not able to make the next connection towards the destination fast enough
- "`Destination host unreachable`" - after a number of timed-out responses the trace will give up

Possible reasons for these errors are bad connections or configuration errors.

For additional troubleshooting, see Troubleshooting Virtual Domains.

Testing traffic from the internal network to the ISP

In this example, a route is traced from the Company A internal network to ISP A. The test was run on a Windows PC with an IP address of 10.11.101.55.

The output here indicates three hops between the source and destination, the IP address of each hop, and that the trace was successful.

From the Company A internal network, access a command prompt and enter this command:

```
C:\>tracert 172.20.201.7
Tracing route to 172.20.201.7 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.11.101.2
  2   <10 ms   <10 ms   <10 ms  172.20.101.2
  3   <10 ms   <10 ms   <10 ms  172.20.201.7
Trace complete.
```

Virtual Domains in Transparent mode

In Transparent mode, the FortiGate unit behaves like a layer-2 bridge but can still provide services such as antivirus scanning, web filtering, spam filtering and intrusion protection to traffic. There are some limitations in Transparent mode in that you cannot use SSL VPN, PPTP/L2TP VPN, DHCP server, or easily perform NAT on traffic. The limits in Transparent mode apply to IEEE 802.1Q VLAN trunks passing through the unit.

VDOMs can each be configured to operate either in Transparent or NAT/Route operation mode, with each VDOM behaving like a separate FortiGate unit operating in the respective mode. VLANs configured on a VDOM in Transparent mode are the same as VLANs configured on the FortiGate unit when VDOMs are disabled.

This chapter includes the following sections:

- Transparent operation mode
- Configuring VDOMs in Transparent mode
- Example of VDOMs in Transparent mode

Transparent operation mode

In transparent mode, the FortiGate unit becomes a layer-2 IP forwarding bridge. This means that Ethernet frames are forwarded based on destination MAC address, and no other routing is performed. All incoming traffic that is accepted by the firewall, is broadcast out on all interfaces.

In transparent mode the FortiGate unit is a forwarding bridge, not a switch. A switch can develop a port table and associated MAC addresses, so that it can bridge two ports to deliver the traffic instead of broadcasting to all ports. In transparent mode, the FortiGate unit does not following this switch behavior, but instead is the forwarding bridge that broadcasts all packets out over all interfaces, subject to security policies.

Features such as broadcast domains, forwarding domains, and STP apply to both FortiGate units and VDOMs in Transparent mode.

Broadcast domains

A broadcast domain is a network segment in which any network equipment can transmit data directly to another device without going through a routing device. All the devices share the same subnet. The subnets are separated by layer-3 devices, such as routers, that can forward traffic from one broadcast domain to the next.

Broadcast domains are important to transparent mode FortiGate units because the broadcast domain is the limit of where the FortiGate unit can forward packets when it is in transparent mode.

Forwarding domains

Address Resolution Protocol (ARP) packets are vital to communication on a network, and ARP support is enabled on FortiGate unit interfaces by default. Normally you want ARP packets to pass through the FortiGate unit. However, in Transparent mode ARP packets arriving on one interface are sent to all other interfaces including VLANs giving the appearance of duplicates of the same MAC address on different interfaces. Some layer-2 switches become unstable when they detect these duplicate MAC addresses. Unstable switches may become unreliable or reset and cause network traffic to slow down considerably.

When you are using VLANs in Transparent mode, the solution to the duplicate MAC address issue is to use the `forward-domain` CLI command. This command tags VLAN traffic as belonging to a particular collision group,

and only VLANs tagged as part of that collision group receive that traffic—it is like an additional set of VLANs. By default, all interfaces and VLANs are part of forward-domain collision group 0.

To assign VLAN 200 to collision group 2, VLAN 300 to collision group 3, and all other interfaces to stay in the default collision group 0 enter the following CLI commands:

```
config system interface
   edit vlan200
      set vlanid 200
      set forward_domain 2
   next
   edit vlan300
      set vlanid 300
      set forward_domain 3
   next
end
```

When using forwarding domains, you may experience connection issues with layer-2 traffic, such as ping, if your network configuration has

- packets going through the FortiGate unit in Transparent mode multiple times,
- more than one forwarding domain (such as incoming on one forwarding domain and outgoing on another)
- IPS and AV enabled.

Spanning Tree Protocol

VDOMs and FortiGate units do not participate in the Spanning Tree Protocol (STP). STP is an IEEE 802.1 protocol that ensures there are no layer-2 loops on the network. Loops are created when there is more than one route for traffic to take and that traffic is broadcast back to the original switch. This loop floods the network with traffic, quickly reducing available bandwidth to zero.

If you use your VDOM or FortiGate unit in a network topology that relies on STP for network loop protection, you need to make changes to your FortiGate configuration. Otherwise, STP recognizes your FortiGate unit as a blocked link and forwards the data to another path. By default, your FortiGate unit blocks STP as well as other non-IP protocol traffic. Using the CLI, you can enable forwarding of STP and other layer-2 protocols through the interface. In this example, layer-2 forwarding is enabled on the port2 interface:

```
config global
   config system interface
      edit port2
         set l2forward enable
         set stpforward enable
      next
   end
```

There are different CLI commands to allow other common layer-2 protocols such as IPX, PPTP or L2TP on the network. For more information, see the FortiOS CLI Reference.

Differences between NAT/Route and Transparent mode

The differences between NAT/Route mode and Transparent mode include:

Differences between NAT/Route and Transparent modes

Features	NAT/Route mode	Transparent mode
Specific Management IP address required	No	Yes
Perform Network Address Translation (NAT)	Yes	Yes
Stateful packet inspection	Yes	Yes
Layer-2 forwarding	Yes	Yes
Layer-3 routing	Yes	No
Unicast Routing / Policy Based routing	Yes	No
DHCP server	Yes	No
IPsec VPN	Yes	Yes
PPTP/L2TP VPN	Yes	No
SSL VPN	Yes	No
Security features	Yes	Yes
VLAN support	Yes	Yes - limited to VLAN trunks.
Ping servers (dead gateway detection)	Yes	No

To provide administrative access to a FortiGate unit or VDOM in Transparent mode, you must define a management IP address and a gateway. This step is not required in NAT/Route mode where you can access the FortiGate unit through the assigned IP address of any interface where administrative access is permitted.

If you incorrectly set the Transparent mode management IP address for your FortiGate unit, you will be unable to access your unit through the web-based manager. In this situation, you will need to connect to the FortiGate unit using the console cable and change the settings so you can access the unit. Alternately, if your unit has an LCD panel, you can change the operation mode and interface information through the LCD panel.

Operation mode differences in VDOMs

A VDOM, such as root, can have a maximum of 255 interfaces in Network Address Translation (NAT) mode or Transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. To have more than a total of 255 interfaces configured, you need multiple VDOMs with multiple interfaces on each.

In Transparent mode without VDOMs enabled, all interfaces on the FortiGate unit act as a bridge — all traffic coming in on one interface is sent back out on all the other interfaces. This effectively turns the FortiGate unit into a two interface unit no matter how many physical interfaces it has. When VDOMs are enabled, this allows you to

determine how many interfaces to assign to a VDOM running in Transparent mode. If there are reasons for assigning more than two interfaces based on your network topology, you are able to. However, the benefit of VDOMs in this case is that you have the functionality of Transparent mode, but you can use interfaces for NAT/Route traffic as well.

You can add more VDOMs to separate groups of VLAN subinterfaces. When using a FortiGate unit to serve multiple organizations, this configuration simplifies administration because you see only the security policies and settings for the VDOM you are configuring. For information on adding and configuring virtual domains, see Benefits of Virtual Domains.

One essential application of VDOMs is to prevent problems caused when a FortiGate unit is connected to a layer-2 switch that has a global MAC table. FortiGate units normally forward ARP requests to all interfaces, including VLAN subinterfaces. It is then possible for the switch to receive duplicate ARP packets on different VLANs. Some layer-2 switches reset when this happens. As ARP requests are only forwarded to interfaces in the same VDOM, you can solve this problem by creating a VDOM for each VLAN. For a configuration example, see Example of VDOMs in Transparent mode.

Configuring VDOMs in Transparent mode

In Transparent mode, your FortiGate unit becomes a layer-2 bridge — any traffic coming in on one port is broadcast out on all the other ports. If your FortiGate unit has many interfaces, this is not the best use of those interfaces. VDOMs can limit Transparent mode to only a few interfaces while allowing the rest of the FortiGate unit to remain in NAT/Route mode.

The essential steps to configure your FortiGate unit to work with VLANs in Transparent mode are:

- Switching to Transparent mode
- Adding VLAN subinterfaces
- Creating security policies

You can also configure the security profiles that manage antivirus scanning, web filtering and spam filtering.

In Transparent mode, you can access the FortiGate web-based manager by connecting to an interface configured for administrative access and using HTTPS to access the management IP address. On the FortiGateunit used for examples in this guide, administrative access is enabled by default on the internal interface and the default management IP address is `10.11.0.1`.

Switching to Transparent mode

A VDOM is in NAT/Route mode by default when it is created. You must switch it to Transparent mode, and add a management IP address so you can access the VDOM from your management computer.

Before applying the change to Transparent mode, ensure the VDOM has administrative access on the selected interface, and that the selected management IP address is reachable on your network.

To switch the `tpVDOM` VDOM to Transparent mode - web-based manager:

1. Go to **Global > VDOM > VDOM**.
2. Edit the **tpVDOM**.
3. Select `Transparent` for **Operation mode**.
4. Enter the management IP/Netmask.
   The IP address must be accessible to the subnet where the management computer is located. For example 10.11.0.99/255.255.255.0 will be able to access the 10.11.0.0 subnet.
5. Select **Apply**.

When you select **Apply**, the FortiGate unit will log you out. When you log back in, the VDOM will be in Transparent mode.

To switch the `tpVDOM` VDOM to Transparent mode - CLI:

```
config vdom
   edit tpVDOM
      config system settings
         set opmode transparent
         set mangeip 10.11.0.99 255.255.255.0
      end
   end
```

Adding VLAN subinterfaces

There are a few differences when adding VLANs in Transparent mode compared to NAT/Route mode.

In Transparent mode, VLAN traffic is trunked across the VDOM. That means VLAN traffic cannot be routed, changed, or inspected. For this reason when you assign a VLAN to a Transparent mode VDOM, you will see the **Addressing Mode** section of the interface configuration disappear in from the web-based manager. It is because with no routing, inspection, or any activities able to be performed on VLAN traffic the VDOM simply re-broadcasts the VLAN traffic. This requires no addressing.

Also any routing related features such as dynamic routing or Virtual Router Redundancy Protocol (VRRP) are not available in Transparent mode for any interfaces.

Creating security policies

Security policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Typically you will also limit communication to desired times and services for additional security.

In Transparent mode, the FortiGate unit performs antivirus and antispam scanning on each packet as it passes through the unit. You need security policies to permit packets to pass from the VLAN interface where they enter the unit to the VLAN interface where they exit the unit. If there are no security policies configured, no packets will be allowed to pass from one interface to another. For more information, see the FortiGate Administration Guide.

Example of VDOMs in Transparent mode

In this example, the FortiGate unit provides network protection to two organizations — Company A and Company B. Each company has different policies for incoming and outgoing traffic, requiring three different security policies and protection profiles.

VDOMs are not required for this configuration, but by using VDOMs the profiles and policies can be more easily managed on a per-VDOM basis either by one central administrator or separate administrators for each company. Also future expansion is simply a matter of adding additional VDOMs, whilst not disrupt the existing VDOMs.

For this example, firewalls are only included to deal with web traffic. This is to provide an example without making configuration unnecessarily complicated.

This example includes the following sections:

- Network topology and assumptions
- General configuration steps
- Configuring common items
- Creating virtual domains
- Configuring the Company_A VDOM
- Configuring the Company_B VDOM
- Virtual Domains in Transparent mode
- Testing the configuration

Network topology and assumptions

Each organization's internal network consists of a different range of IP addresses:

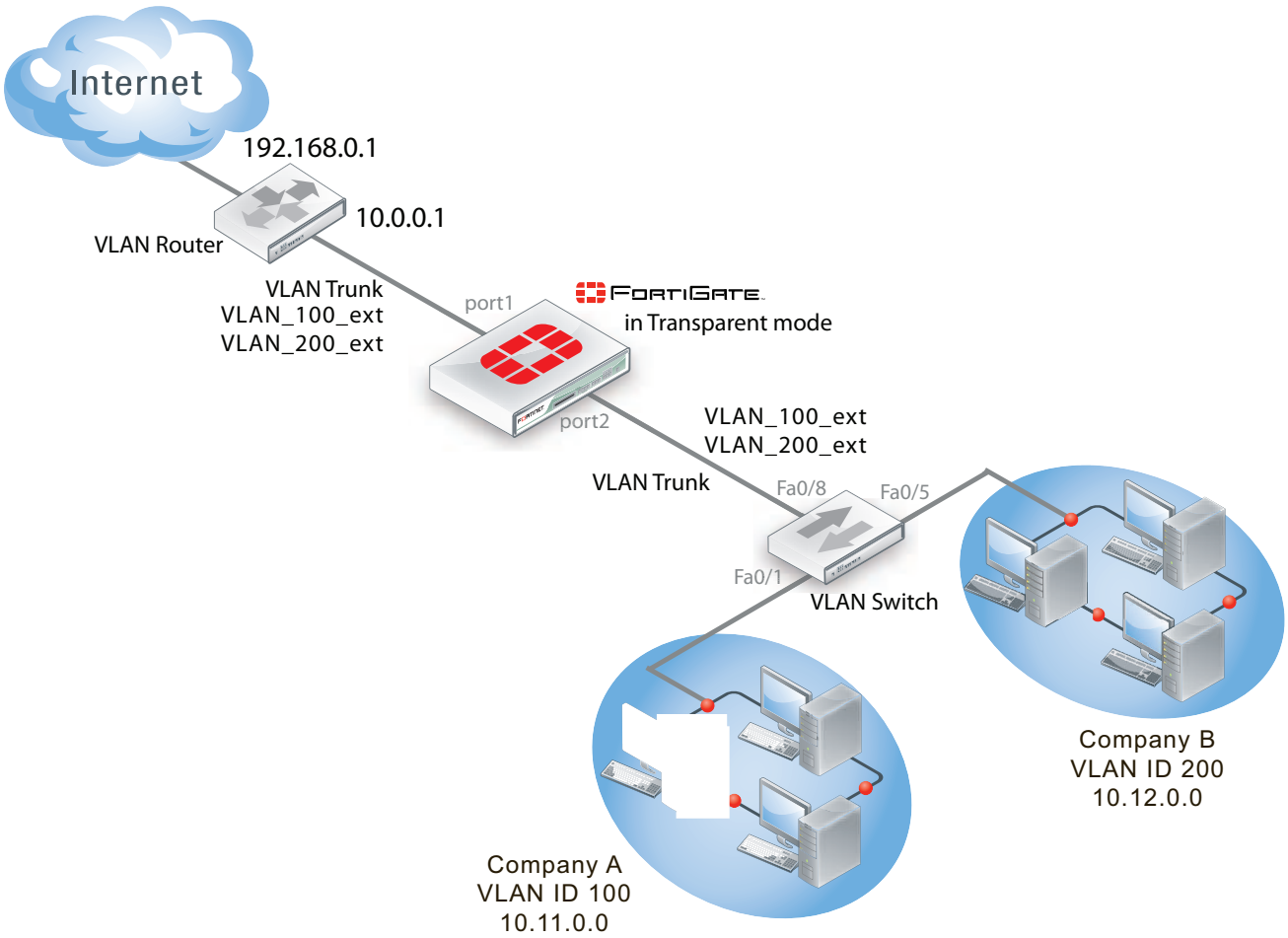
- 10.11.0.0/255.255.0.0 for Company A.
- 10.12.0.0/255.255.0.0 for Company B.

For the procedures in this section, it is assumed that you have enabled VDOM configuration on your FortiGate unit. For more information, see Enabling and accessing Virtual Domains.

The VDOM names are similar to the company names for easy recognition. The root VDOM cannot be renamed and is not used in this example.

Interfaces used in this example are port1 and port2. Some FortiGate models may not have interfaces with these names. port1 is an external interface. port2 is an internal interface.

Figure 10: VLAN and VDOM Transparent example network topology



General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring common items
2. Creating virtual domains
3. Configuring the Company_A VDOM
4. Configuring the Company_B VDOM
5. Virtual Domains in Transparent mode
6. Testing the configuration

Configuring common items

Both VDOMs require you configure security profiles. These will be configured the same way, but need to be configured in both VDOMs.

The relaxed profile allows users to surf websites they are not allowed to visit during normal business hours. Also a quota is in place to restrict users to one hour of access to these websites to ensure employees do not take long and unproductive lunches.

To create a strict web filtering profile - web-based manager:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter > Profile**.
2. Select **Create New**.
3. Enter `strict` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for all Categories except Business Oriented, and Other.
5. Block all Classifications except Cached Content, and Image Search.
6. Ensure **FortiGuard Quota** for all Categories and Classifications is Disabled.
7. Select **OK**.

To create a strict web filtering profile - CLI:

```
config vdom
   edit <vdom_name>
      config webfilter profile
         edit strict
            config ftgd-wf
               set allow g07 g08 g21 g22 c01 c03
               set deny g01 g02 g03 g04 g05 g06 c02 c04 c05 c06 c07
            end
            set web-ftgd-err-log enable
         end
```

To create a relaxed web filtering profile - web-based manager:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter > Profile**.
2. Select **Create New**.
3. Enter `relaxed` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for Potentially Security Violating Category, and Spam URL Classification.
5. Enable FortiGuard Quotas to allow 1 hour for all allowed Categories and Classifications.

Creating virtual domains

The FortiGate unit supports 10 virtual domains. Root is the default VDOM. It cannot be deleted or renamed. The root VDOM is not used in this example. New VDOMs are created for Company A and Company B

To create the virtual domains - web-based manager:

1. With VDOMs enabled, select **System > VDOM > VDOM**.
2. Select **Create New**.
3. Enter `Company_A` for Name, and select **OK**.
4. Select **Create New**.
5. Enter `Company_B` for Name, and select **OK**.

To create the virtual domains - CLI:

```
config system vdom
   edit Company_A
   next
   edit Company_B
end
```

Configuring the Company_A VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company_A VDOM.

This section includes the following topics:

- Adding VLAN subinterfaces
- Creating the Lunch schedule
- Configuring Company_A firewall addresses
- Creating Company_A security policies

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the port2 interface and another one on the port1 interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager:

1. Go to **System > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100_int
Interface	port2
VLAN ID	100
Virtual Domain	Company_A

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_100_ext
Interface	port1
VLAN ID	100
Virtual Domain	Company_A

To add the VLAN subinterfaces - CLI:

```
config system interface
```

```
edit VLAN_100_int
   set interface port2
   set vlanid 100
   set vdom Company_A
next
edit VLAN_100_ext
   set interface port1
   set vlanid 100
   set vdom Company_A
end
```

Creating the Lunch schedule

Both organizations have the same lunch schedule, but only Company A has relaxed its security policy to allow employees more freedom in accessing the Internet during lunch. Lunch schedule will be Monday to Friday from 11:45am to 2:00pm (14:00).

To create a recurring schedule for lunchtime - web-based manager:

1. In Company_A VDOM, go to **Firewall Objects > Schedule > Recurring**.
2. Select **Create New**.
3. Enter `Lunch` as the name for the schedule.
4. Select **Mon**, **Tues**, **Wed**, **Thu**, and **Fri**.
5. Set the **Start** time as `11:45` and set the **Stop** time as `14:00`.
6. Select **OK**.

To create a recurring schedule for lunchtime - CLI:

```
config vdom
   edit Company_A
      config firewall schedule recurring
         edit Lunch
            set day monday tuesday wednesday thursday friday
            set start 11:45
            set end 14:00
         end
```

Configuring Company_A firewall addresses

For Company A, its networks are all on the 10.11.0.0 network, so restricting addresses to that domain provides added security.

To configure Company_A firewall addresses - web-based manager:

1. In the Company_A VDOM, go to **Firewall Objects > Address > Address**.
2. Select **Create New**.
3. Enter `CompanyA` in the **Address Name** field.
4. Type 10.11.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure vdomA firewall addresses - CLI:

```
config firewall address
   edit CompanyA
      set type ipmask
      set subnet 10.11.0.0 255.255.0.0
   end
```

Creating Company_A security policies

A security policy can include varying levels of security feature protection. This example only deals with web filtering. The following security policies use the custom security `strict` and `relaxed` profiles configured earlier. See Configuring common items.

For these security policies, we assume that all protocols will be on their standard ports, such as port 80 for http traffic. If the ports are changed, such as using port 8080 for http traffic, you will have to create custom services for protocols with non-standard ports, and assign them different names.

The firewalls configured in this section are:

- internal to external — always deny all
- external to internal — always deny all
- internal to external — always allow all, security features - web filtering: strict
- internal to external — Lunch allow all, security features - web filtering:relaxed

Security policies allow packets to travel between the internal VLAN_100 interface to the external interface subject to the restrictions of the protection profile. Entering the policies in this order means the last one configured is at the top of the policy list, and will be checked first. This is important because the policies are arranged so if one does not apply the next is checked until the end of the list.

To configure Company_A security policies - web-based manager:

1. Go to **Policy > Policy**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_100_int
Source Address	CompanyA
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	always
Service	all
Action	DENY

This policy is a catch all for outgoing traffic to ensure that if it doesn't match any of the other policies, it will not be allowed. This is standard procedure.

4. Select **Create New**.
5. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_100_ext
Source Address	all
Destination Interface/Zone	VLAN_100_int
Destination Address	CompanyA
Schedule	always
Service	all
Action	DENY

This policy is a catch all for incoming traffic to ensure that if it doesn't match any of the other policies, it will not be allowed. This is standard procedure.

6. Select **Create New**.
7. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_100_int
Source Address	CompanyA
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	always
Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	strict

This policy enforces strict scanning at all times, while allowing all traffic. It ensures company policies are met for network security.

8. Select **Create New**.
9. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_100_int
Source Address	CompanyA
Destination Interface/Zone	VLAN_100_ext

Destination Address	all
Schedule	Lunch
Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	relaxed

This policy provides relaxed protection during lunch hours — going from strict down to scan for protocol options and web filtering. AntiVirus and Email Filtering remain at strict for security — relaxing them would not provide employees additional access to the Internet and it would make the company vulnerable.

10. Verify that the policies entered appear in the list with the last policy (lunch) at the top, and the first policy (deny all) at the bottom. Otherwise traffic will not flow as expected.

To configure Company_A security policies - CLI:

```
config vdom
   edit Company_A
      config firewall policy
         edit 1
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule Lunch
            set webfiltering relaxed
         next
         edit 3
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule BusinessDay
            set service HTTP
            set profile_status enable
            set profile BusinessOnly
         end
```

Configuring the Company_B VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company B VDOM.

This section includes the following topics:

- Adding VLAN subinterfaces
- Creating Company_B service groups

- Configuring Company_B firewall addresses
- Configuring Company_B security policies

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager:

1. Go to **System > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_200_int
Interface	port2
VLAN ID	200
Virtual Domain	Company_B

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_200_ext
Interface	port1
VLAN ID	200
Virtual Domain	Company_B

To add the VLAN subinterfaces - CLI:

```
config system interface
   edit VLAN_200_int
      set interface internal
      set vlanid 200
      set vdom Company_B
   next
   edit VLAN_200_ext
      set interface external
      set vlanid 200
      set vdom Company_B
   end
```

Creating Company_B service groups

Company_B does not want its employees to use any online chat software except NetMeeting, which the company uses for net conferencing. To simplify the creation of a security policy for this purpose, you create a service group that contains all of the services you want to restrict. A security policy can manage only one service or one group.

To create a chat service group - web-based manager:

1. Go to **Firewall Objects > Service > Groups**.
2. Select **Create New**.
3. Enter `Chat` in the **Group Name** field.
4. For each of IRC, AOL, SIP-MSNmessenger and TALK, select the service in the **Available Services** list and select the right arrow to add it to the **Members** list.

If a particular service does not appear in the **Available Services** list, see the list in **Firewall Objects > Service > Services**. Some services do not appear by default unless edited.

5. Select **OK**.

To create a games and chat service group - CLI:

```
config firewall service group
   edit Chat
      set member IRC SIP-MSNmessenger AOL TALK
   end
```

Configuring Company_B firewall addresses

Company B's network is all in the 10.12.0.0 network. Security can be improved by only allowing traffic from IP addresses on that network.

To configure Company_B firewall address - web-based manager:

1. In the Company_B VDOM, go to **Firewall Objects > Address > Address.**
2. Select **Create New**.
3. Enter `new` in the **Address Name** field.
4. Type 10.12.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure Company_B firewall addresses - CLI:

```
config vdom
   edit Company_B
      config firewall address
         edit all
            set type ipmask
            set subnet 10.12.0.0 255.255.0.0
         end
```

Configuring Company_B security policies

Security policies allow packets to travel between the internal and external VLAN_200 interfaces subject to the restrictions of the protection profile.

To configure Company_B security policies - web-based manager:

1. Go to **Policy > Policy**.
2. Select **Create New**.

3. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	BusinessDay
Service	games-chat
Action	DENY

This policy prevents the use of network games or chat programs (except NetMeeting) during business hours.

4. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	Lunch
Service	HTTP
Action	ACCEPT
Protection Profile	Relaxed

This policy relaxes the web category filtering during lunch hour.

5. Select **Create New**.
6. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	BusinessDay
Service	HTTP

Action	ACCEPT
Protection Profile	BusinessOnly

This policy provides rather strict web category filtering during business hours.

7. Select **Create New**.
8. Enter the following information and select **OK**:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	always
Service	ANY
Action	ACCEPT
Protection Profile	Relaxed

Because it is last in the list, this policy applies to the times and services not covered in preceding policies. This means that outside of regular business hours, the Relaxed protection profile applies to email and web browsing, and online chat and games are permitted. Company B needs this policy because its employees sometimes work overtime. The other companies in this example maintain fixed hours and do not want any after-hours Internet access.

To configure Company_B security policies - CLI:

```
config firewall policy
   edit 1
      set srcintf VLAN_200_int
      set srcaddr all
      set dstintf VLAN_200_ext
      set dstaddr all
      set schedule BusinessDay
      set service Games
      set action deny
   next
   edit 2
      set srcintf VLAN_200_int
      set srcaddr all
      set dstintf VLAN_200_ext
      set dstaddr all
      set action accept
      set schedule Lunch
      set service HTTP
      set profile_status enable
      set profile Relaxed
   next
   edit 3
```

```
        set srcintf VLAN_200_int
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule BusinessDay
        set service HTTP
        set profile_status enable
        set profile BusinessOnly
    next
    edit 4
        set srcintf VLAN_200_int
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule always
        set service ANY
        set profile_status enable
        set profile Relaxed
    end
```

Testing the configuration

Use diagnostic commands, such as tracert, to test traffic routed through the network.

You should test traffic between the internal VLANs as well as from the internal VLANs to the Internet to ensure connectivity.

For additional troubleshooting, see Troubleshooting Virtual Domains.

This section includes the following topics:

- Testing traffic from VLAN_100 to the Internet
- Testing traffic from VLAN_100 to VLAN_200

Testing traffic from VLAN_100 to the Internet

In this example, a route is traced from VLANs to a host on the Internet. The route target is www.example.com.

From a host on VLAN_100, access a command prompt and enter this command:

```
C:\>tracert www.example.com
Tracing route to www.example.com [208.77.188.166]
over a maximum of 30 hops:
 1 <10 ms <10 ms <10 ms 10.100.0.1
...
14 172 ms 141 ms 140 ms 208.77.188.166
Trace complete.
```

The number of steps between the first and the last hop, as well as their IP addresses, will vary depending on your location and ISP. However, all successful tracerts to www.example.com will start and end with these lines.

Repeat the tracert for VLAN_200.

The tracert for each VLAN will include the gateway for that VLAN as the first step. Otherwise, the tracert should be the same for each VLAN.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.12.0.2
Tracing route to 10.12.0.2 over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 10.100.0.1
2 <10 ms <10 ms <10 ms 10.12.0.2
Trace complete.
```

You can repeat this for different routes in the topology. In each case the IP addresses will be the gateway for the starting VLAN, and the end point at the ending VLAN.

Inter-VDOM routing

In the past, virtual domains (VDOMs) were separate from each other—there was no internal communication. Any communication between VDOMs involved traffic leaving on a physical interface belonging to one VDOM and re-entering the FortiGate unit on another physical interface belonging to another VDOM to be inspected by firewall policies in both directions.

Inter-VDOM routing changes this. With VDOM links, VDOMs can communicate internally without using additional physical interfaces.

Inter-VDOM routing is the communication between VDOMs. VDOM links are virtual interfaces that connect VDOMs. A VDOM link contains a pair of interfaces with each one connected to a VDOM, and forming either end of the inter-VDOM connection.

This chapter contains the following sections:

- Benefits of inter-VDOM routing
- Getting started with VDOM links
- Dynamic routing over inter-VDOM links
- HA virtual clusters and VDOM links
- Example of inter-VDOM routing

Benefits of inter-VDOM routing

Inter-VDOM routing has a number of advantages over independent VDOM routing. These benefits include:

- Freed-up physical interfaces
- More speed than physical interfaces
- Continued support for secure firewall policies
- Configuration flexibility

Freed-up physical interfaces

Tying up physical interfaces on the FortiGate unit presents a problem. With a limited number of interfaces available, configuration options for the old style of communication between VDOMs are very limited. VLANs can be an answer to this, but they have some limitations.

For example, the FortiGate-800 has 8 physical ethernet ports. If they are assigned 2 per VDOM (one each for external and internal traffic) there can only be 4 VDOMs at most configured, not the 10 VDOMs the license will allow. Adding even one additional interface per VDOM to be used to communicate between VDOMs leaves only 2 VDOMs for that configuration, since it would required 9 interfaces for 3 VDOMs. Even using one physical interface for both external traffic and inter-VDOM communication would severely lower the available bandwidth for external traffic on that interface.

With the introduction of inter-VDOM routing, traffic can travel between VDOMs internally, freeing up physical interfaces for external traffic. Using the above example we can use the 4 VDOM configuration and all the interfaces will have their full bandwidth.

More speed than physical interfaces

Internal interfaces are faster than physical interfaces. Their speed depends on the FortiGate unit CPU and its load. That means that an inter-VDOM link interface will be faster than a outbound physical interface connected to another inbound physical interface.

Inter-VDOM links are CPU bound, and cannot be part of an accelerated pair of interfaces.

However, while one virtual interface with normal traffic would be considerably faster than on a physical interface, the more traffic and more internal interfaces you configure, the slower they will become until they are slower than the physical interfaces. CPU load can come from other sources such as AV or content scanning. This produces the same effect—internal interfaces such as inter-VDOM links will be slower.

Continued support for secure firewall policies

VDOMs help to separate traffic based on your needs. This is an important step in satisfying regulations that require proof of secure data handling. This is especially important to health, law, accounting, and other businesses that handle sensitive data every day.

By keeping things separate, traffic has to leave the FortiGate unit and re-enter to change VDOMs. This forces traffic to go through the firewall when leaving and enter through another firewall, keeping traffic secure.

With inter-VDOM routing, the need for the physical interfaces is greatly reduced. However, firewall policies still need to be in place for traffic to pass through any interface, physical or virtual, and thus provide the same level of security both internally and externally. Configuration of firewall policies is the same for inter-VDOM links as for any other interface, and your data will continue to have the high level of security.

Configuration flexibility

A typical VDOM uses at least two interfaces, typically physical interfaces, one for internal and one for external traffic. Depending on the configuration, more interfaces may be required. This means that the maximum number of VDOMs configurable on a FortiGate unit using physical interfaces is the number of interfaces available divided by two. VLANs can increase the number by providing multiple virtual interfaces over a single physical interface, but VLANs have some limitations. Using physical interfaces for inter-VDOM communication therefore limits the number of possible configurations on your FortiGate unit.

To overcome this limitation, inter-VDOM links can be created within the FortiGate unit. Using virtual interfaces, inter-VDOM links free up the physical interfaces for external traffic. Using VDOM links on a FortiGate unit with 8 physical interfaces, you can have 4 VDOMs communicating with each other (meshed configuration) and continue to have 2 physical interfaces each for internal and external connections. This configuration would have required 20 physical interfaces without inter-VDOM routing. With inter-VDOM routing it only requires 8 physical interfaces, with the other 12 interfaces being internal VDOM links.

Inter-VDOM routing allows you to make use of Standalone VDOM configuration, Management VDOM configuration, and Meshed VDOM configuration without being limited by the number of physical interfaces on your FortiGate unit.

Getting started with VDOM links

Once VDOMs are configured on your FortiGate unit, configuring inter-VDOM routing and VDOM-links is very much like creating a VLAN interface. VDOM-links are managed through the web-based manager or CLI. In the web-based manager, VDOM link interfaces are managed in the network interface list.

This section includes the following topics:

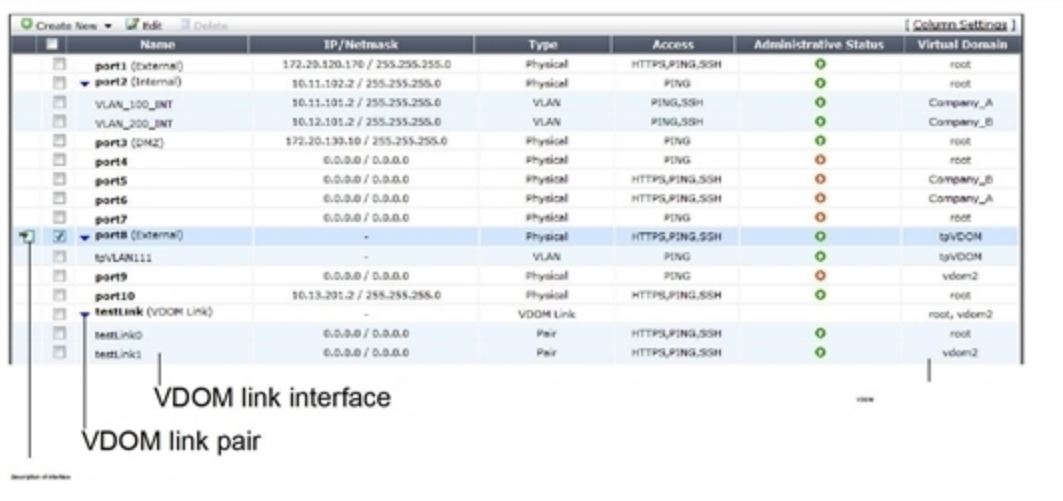
- Viewing VDOM links
- Creating VDOM links
- Deleting VDOM links
- NAT to Transparent VDOM links

Viewing VDOM links

VDOM links are displayed on the network interface list in the web-based manager. You can view VDOM links only if you are using a super_admin account and in global configuration.

To view the network interface list, in the Global menu go to **System > Network > Interfaces.**

Interface list displaying interface names and information



Create New	Select the arrow to create a new interface or VDOM link. Interface options include VLAN, Aggregate, Redundant, or loopback interfaces. For more information, see Creating VDOM links.
Edit	Select to change interface configuration for the selected interface. This option not available if no interfaces or multiple interfaces are selected.
Delete	Select to remove an interface from the list. One or more interfaces must be selected for this option to be available. You cannot delete permanent physical interfaces, or any interfaces that have configuration referring to them. See Deleting VDOM links or see Deleting an interface.
Column Settings	Select to change which information is displayed about the interfaces, and in which order the columns appear. Use to display VDOM, VLAN, and other information.
Checkbox	Select the checkbox for an interface to edit or delete that interface. Select multiple interfaces to delete those interfaces. Optionally select the check box at the top of the column to select or unselect all checkboxes.
Name	The name of the interface. The name of the VDOM link (`vlink1`) has an expand arrow to display or hide the pair of VDOM link interfaces. For more information, see Viewing VDOM links.
IP/Netmask	The IP address and netmask assigned to this interface.
Type	The type of interface such as physical, VLAN, or VDOM link pair.
Access	The protocols allowed for administrators to connect to the FortiGate unit.
Administrative Status	The status of this interface, either set to up (active) or down (disabled).
Virtual Domain	The virtual domain this interface belongs to. For more information on VDOMs, see Virtual Domains in NAT/Route mode.

Creating VDOM links

VDOM links connect VDOMs together to allow traffic to pass between VDOMs as per firewall policies. Inter-VDOM links are virtual interfaces that are very similar to VPN tunnel interfaces except inter-VDOM links do not require IP addresses. See IP addresses and inter-VDOM links.

To create a VDOM link, you first create the point-to-point interface, and then bind the two interface objects associated with it to the virtual domains.

In creating the point-to-point interface, you also create two additional interface objects by default. They are called `vlink10` and `vlink11` - the interface name you chose with a 1 or a 0 to designate the two ends of the link.

Once the interface objects are bound, they are treated like normal FortiGate interfaces and need to be configured just like regular interfaces.

The assumptions for this example are as follows:

- Your FortiGate unit has VDOMs enabled and you have 2 VDOMs called `customer1` and `customer2` already configured. For more information on configuring VDOMs see Configuring Virtual Domains.
- You are using a super_admin account

To configure an inter-VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New > VDOM link**, enter the following information, and select **OK**.

Name		vlink1 (The name can be up to 11 characters long. Valid characters are letters, numbers, "-", and "_". No spaces are allowed.)
Interface #0		
	Virtual Domain	customer1
	IP/Netmask	10.11.12.13/255.255.255.0
	Administrative Access	HTTPS, SSL
Interface #1		
	Virtual Domain	customer2
	IP/Netmask	172.120.100.13/255.255.255.0
	Administrative Access	HTTPS, SSL

To configure an inter-VDOM link - CLI:

```
config global
   config system vdom-link
      edit vlink1
      end
   config system interface
      edit vlink10
         set vdom customer1
      next
      edit vlink11
         set vdom customer2
      end
```

Once you have created and bound the interface ends to VDOMs, configure the appropriate firewall policies and other settings that you require. To confirm the inter-VDOM link was created, find the VDOM link pair and use the expand arrow to view the two VDOM link interfaces. You can select edit to change any information.

IP addresses and inter-VDOM links

Besides being virtual interfaces, here is one main difference between inter-VDOM links and regular interfaces—default inter-VDOM links do not require IP addresses. IP addresses are not required by default because an inter-VDOM link is an internal connection that can be referred to by the interface name in firewall policies, and other system references. This introduces three possible situations with inter-VDOM links that are:

- **unnumbered** - an inter-VDOM link with no IP addresses for either end of the tunnel
- **half numbered** - an inter-VDOM link with one IP address for one end and none for the other end
- **full numbered** - an inter-VDOM link with two IP addresses, one for each end.

Not using an IP address in the configuration can speed up and simplify configuration for you. Also you will not use up all the IP addresses in your subnets if you have many inter-VDOM links.

Half or full numbered interfaces are required if you are doing NAT, either SNAT or DNAT as you need an IP number on both ends to translate between.

You can use unnumbered interfaces in static routing, by naming the interface and using `0.0.0.0` for the gateway. Running traceroute will not show the interface in the list of hops. However you can see the interface when you are sniffing packets, which is useful for troubleshooting.

Deleting VDOM links

When you delete the VDOM link, the two link objects associated with it will also be deleted. You cannot delete the objects by themselves. The example uses a VDOM routing connection called “vlink1”. Removing vlink1 will also remove its two link objects vlink10 and vlink11.

Before deleting the VDOM link, ensure all policies, firewalls, and other configurations that include the VDOM link are deleted, removed, or changed to no longer include the VDOM link.

To remove a VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Delete** for the VDOM link **vlink1**.

To remove a VDOM link - CLI:

```
config global
   config system vdom-link
      delete vlink1
   end
```

For more information, see the FortiGate CLI Reference.

NAT to Transparent VDOM links

Inter-VDOM links can be created between VDOMs in NAT mode and VDOMs in Transparent mode, but it must be done through the CLI, as the VDOM link type must be changed from the default PPP to Ethernet for the two VDOMs to communicate. The below example assumes one vdom is in NAT mode and one is Transparent.

An IP address must be assigned to the NAT VDOM's interface, but no IP address should be assigned to the Transparent VDOM's interface.

To configure a NAT to Transparent VDOM link - CLI:

```
config global
   config system vdom-link
      edit vlink1
      set type ethernet
      end
   config system interface
      edit vlink10
         set vdom (interface 1 name)
         set ip (interface 1 ip)
      next
      edit vlink11
         set vdom (interface 2 name)
      end
```

Ethernet-type is not recommended for standard NAT to NAT inter-VDOM links, as the default PPP-type link does not require the VDOM links to have addresses, while Ethernet-type does. VDOM link addresses are explained in IP addresses and inter-VDOM links.

Inter-VDOM configurations

By using fewer physical interfaces to inter-connect VDOMs, inter-VDOM links provide you with more configuration options.

None of these configurations use VLANs to reduce the number of physical interfaces. It is generally assumed that an internal or client network will have its own internal interface and an external interface to connect to its ISP and the Internet.

These inter-VDOM configurations can use any FortiGate model with possible limitations based on the number of physical interfaces. VLANs can be used to work around these limitations.

In the following inter-VDOM diagrams, red indicates the physical FortiGate unit, grey indicate network connections external to the FortiGate unit, and black is used for inter-VDOM links and VDOMs.

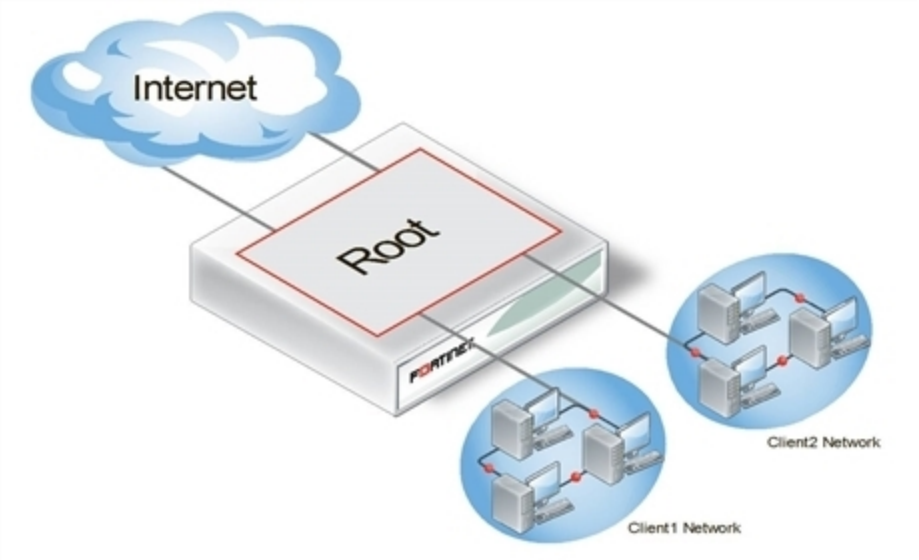
This section includes the following topics:

- Standalone VDOM configuration
- Independent VDOMs configuration
- Management VDOM configuration
- Meshed VDOM configuration

Standalone VDOM configuration

The standalone VDOM configuration uses a single VDOM on your FortiGate unit — the root VDOM that all FortiGate units have by default. This is the VDOM configuration you are likely familiar with. It is the default configuration for FortiGate units before you create additional VDOMs.

Standalone VDOM



The configuration shown above has no VDOM inter-connections and requires no special configurations or settings.

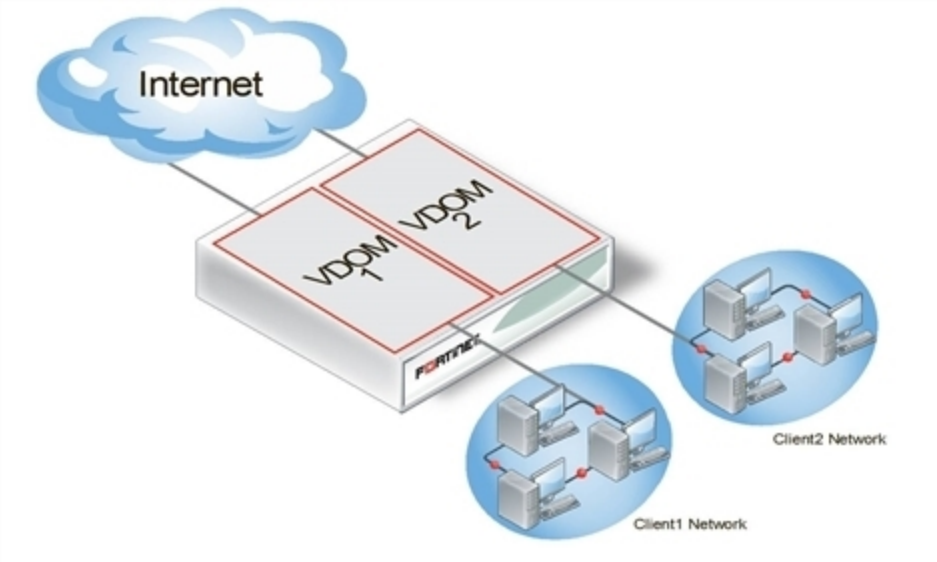
The standalone VDOM configuration can be used for simple network configurations that only have one department or one company administering the connections, firewalls and other VDOM-dependent settings.

However, with this configuration, keeping client networks separate requires many interfaces, considerable firewall design and maintenance, and can quickly become time consuming and complex. Also, configuration errors for one client network can easily affect other client networks, causing unnecessary network downtime.

Independent VDOMs configuration

The independent VDOMs configuration uses multiple VDOMs that are completely separate from each other. This is another common VDOM configuration.

Independent VDOMs



This configuration has no communication between VDOMs and apart from initially setting up each VDOM, it requires no special configurations or settings. Any communication between VDOMs is treated as if communication is between separate physical devices.

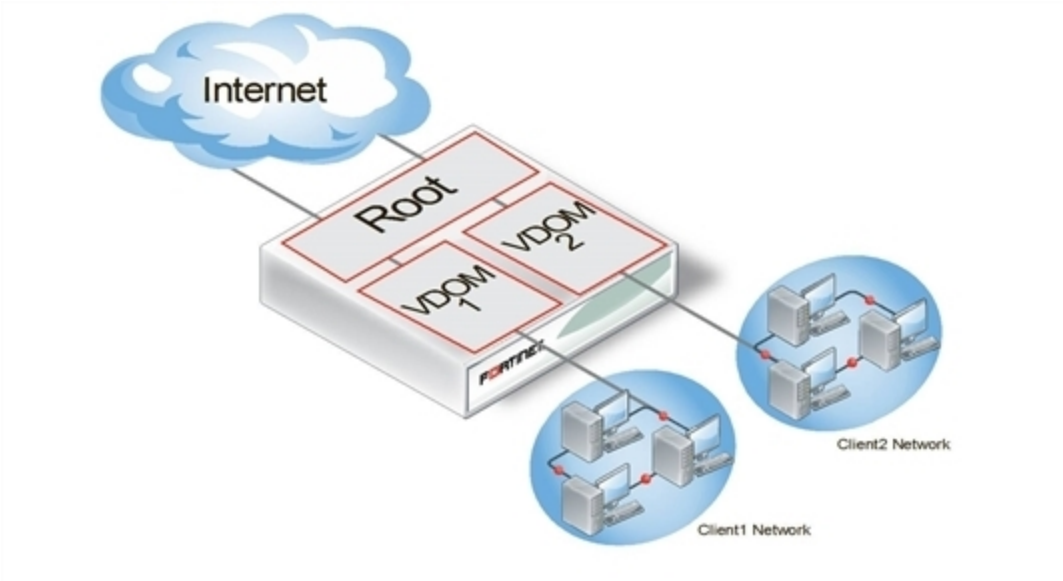
The independent inter-VDOM configuration can be used where more than one department or one company is sharing the FortiGate unit. Each can administer the connections, firewalls and other VDOM-dependent settings for only its own VDOM. To each company or department, it appears as if it has its own FortiGate unit. This configuration reduces the amount of firewall configuration and maintenance required by dividing up the work.

However, this configuration lacks a management VDOM for VDOMs 1, 2, and 3. This is illustrated in Figure 50. This management VDOM would enable an extra level of control for the FortiGate unit administrator, while still allowing each company or department to administer its own VDOM.

Management VDOM configuration

In the management VDOM configuration, the root VDOM is the management VDOM. The other VDOMs are connected to the management VDOM with inter-VDOM links. There are no other inter-VDOM connections.

Management VDOM configuration



The inter-VDOM links connect the management VDOM to the other VDOMs. This does not require any physical interfaces, and the bandwidth of inter-VDOM links can be faster than physical interfaces, depending on the CPU workload.

Only the management VDOM is connected to the Internet. The other VDOMs are connected to internal networks. All external traffic is routed through the management VDOM using inter-VDOM links and firewall policies between the management VDOM and each VDOM. This ensures the management VDOM has full control over access to the Internet, including what types of traffic are allowed in both directions. There is no communication directly between the non-root VDOMs. Security is greatly increased with only one point of entry and exit. Only the management VDOM needs to be fully managed to ensure network security in this case. Each client network can manage its own configuration without compromising security or bringing down another client network.

The management VDOM configuration is ideally suited for a service provider business. The service provider administers the management VDOM with the other VDOMs as customers. These customers do not require a dedicated IT person to manage their network. The service provider controls the traffic and can prevent the customers from using banned services and prevent Internet connections from initiating those same banned services. One example of a banned service might be Instant Messaging (IM) at a company concerned about intellectual property. Another example could be to limit bandwidth used by file-sharing applications without banning that application completely. Firewall policies control the traffic between the customer VDOM and the management VDOM and can be customized for each customer.

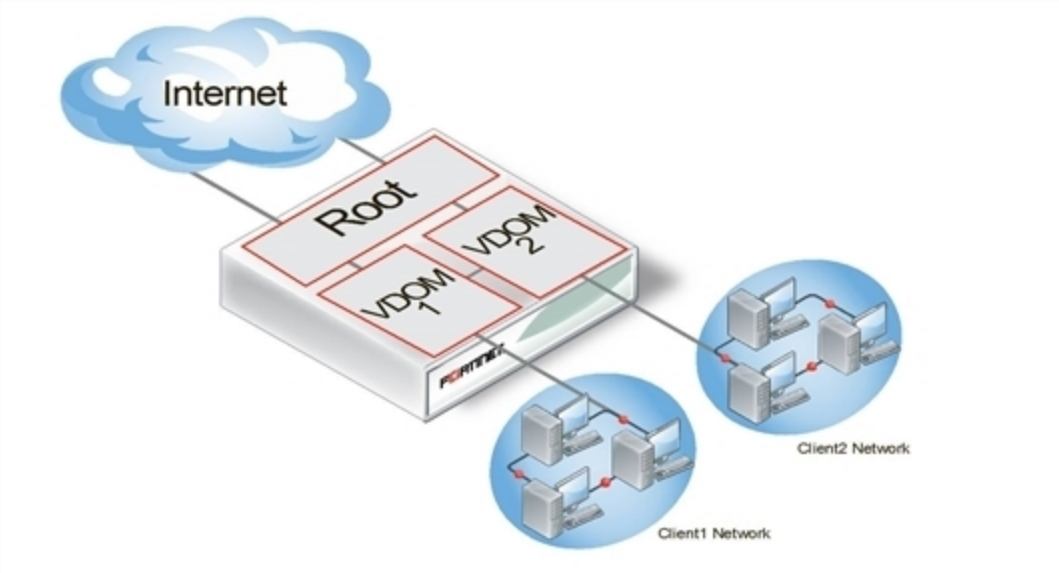
The management VDOM configuration is limited in that the customer VDOMs have no inter-connections. In many situations this limitation is ideal because it maintains proper security. However, some configurations may require customers to communicate with each other, which would be easier if the customer VDOMs were inter-connected.

Meshed VDOM configuration

The meshed VDOMs configuration, including partial and full mesh, has VDOMs inter-connected with other VDOMs. There is no special feature to accomplish this—they are just complex VDOM configurations.

Partial mesh means only some VDOMs are inter-connected. In a full mesh configuration, all VDOMs are inter-connected to all other VDOMs. This can be useful when you want to provide full access between VDOMs but handle traffic differently depending on which VDOM it originates from or is going to.

Meshed VDOMs



With full access between all VDOMs being possible, it is extra important to ensure proper security. You can achieve this level of security by establishing extensive firewall policies and ensuring secure account access for all administrators and users.

Meshed VDOM configurations can become complex very quickly, with full mesh VDOMs being the most complex. Ensure this is the proper solution for your situation before using this configuration. Generally, these configurations are seen as theoretical and are rarely deployed in the field.

Dynamic routing over inter-VDOM links

BGP is supported over inter-VDOM links. Unless otherwise indicated, routing works as expected over inter-VDOM links.

If an inter-VDOM link has no assigned IP addresses to it, it may be difficult to use that interface in dynamic routing configurations. For example BGP requires an IP address to define any BGP router added to the network.

In OSPF, you can configure a router using a router ID and not its IP address. In fact, having no IP address avoids possible confusing between which value is the router ID and which is the IP address. However for that router to become adjacent with another OSPF router it will have to share the same subnet, which is technically impossible without an IP address. For this reason, while you can configure an OSPF router using an IP-less inter-VDOM link, it will likely be of limited value to you.

In RIP the metric used is hop count. If the inter-VDOM link can reach other nodes on the network, such as through a default route, then it may be possible to configure a RIP router on an inter-VDOM link. However, once again it may be of limited value due to limitations.

As stated earlier, BGP requires an IP address to define a router — an IP-less inter-VDOM link will not work with BGP.

In Multicast, you can configure an interface without using an IP address. However that interface will be unable to become an RP candidate. This limits the roles available to such an interface.

HA virtual clusters and VDOM links

FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewall, VPN, IPS, virus scanning, web filtering, and spam filtering.

Virtual clustering extends HA features to provide failover protection and load balancing for a FortiGate unit operating with virtual domains. A virtual cluster consists of a cluster of two FortiGate units operating with virtual domains. Traffic on different virtual domains can be load balanced between the cluster units.

With virtual clusters (vclusters) configured, inter-VDOM links must be entirely within one vcluster. You cannot create links between vclusters, and you cannot move a VDOM that is linked into another virtual cluster. If your FortiGate units are operating in HA mode, with multiple vclusters when you create the vdom-link, the CLI command `config system vdom-link` includes an option to set which vcluster the link will be in.

What is virtual clustering?

Virtual clustering is an extension of the FGCP for FortiGate units operating with multiple VDOMS enabled. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a VDOM operating on two different cluster units. You can also operate virtual clustering in active-active mode to use HA load balancing to load balance sessions between cluster units. Alternatively, by distributing VDOM processing between the two cluster units you can also configure virtual clustering to provide load balancing by distributing sessions for different VDOMs to each cluster unit.

Virtual clustering and failover protection

Virtual clustering operates on a cluster of two (and only two) FortiGate units with VDOMs enabled. Each VDOM creates a cluster between instances of the VDOMs on the two FortiGate units in the virtual cluster. All traffic to and from the VDOM stays within the VDOM and is processed by the VDOM. One cluster unit is the primary unit for each VDOM and one cluster unit is the subordinate unit for each VDOM. The primary unit processes all traffic for the VDOM. The subordinate unit does not process traffic for the VDOM. If a cluster unit fails, all traffic fails over to the cluster unit that is still operating.

Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Virtual clustering and HA override

For a virtual cluster configuration, override is enabled by default for both virtual clusters when you:

- Enable VDOM portioning from the web-based manager by moving virtual domains to virtual cluster 2
- Enter set vcluster2 enable from the CLI config system ha command to enable virtual cluster 2.

Usually you would enable virtual cluster 2 and expect one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. For this distribution to occur override must be enabled for both virtual clusters. Otherwise you will need to restart the cluster to force it to renegotiate.

Virtual clustering and load balancing or VDOM partitioning

There are two ways to configure load balancing for virtual clustering. The first is to set the HA mode to active-active. The second is to configure VDOM partitioning. For virtual clustering, setting the HA Mode to active-active has the same result as active-active HA for a cluster without virtual domains. The primary unit receives all sessions and load balances them among the cluster units according to the load balancing schedule. All cluster units process traffic for all virtual domains.

Note: If override is enabled the cluster may renegotiate too often. You can choose to disable override at any time. If you decide to disable override, for best results, you should disable it for both cluster units.

In a VDOM partitioning virtual clustering configuration, the HA mode is set to active-passive. Even though virtual clustering operates in active-passive mode you can configure a form of load balancing by using VDOM partitioning to distribute traffic between both cluster units. To configure VDOM partitioning you set one cluster unit as the primary unit for some virtual domains and you set the other cluster unit as the primary unit for other virtual domains. All traffic for a virtual domain is processed by the primary unit for that virtual domain. You can control the distribution of traffic between the cluster units by adjusting which cluster unit is the primary unit for each virtual domain.

For example, you could have 4 VDOMs, two of which have a high traffic volume and two of which have a low traffic volume. You can configure each cluster unit to be the primary unit for one of the high volume VDOMs and one of the low volume VDOMs. As a result each cluster unit will be processing traffic for a high volume VDOM and a low volume VDOM, resulting in an even distribution of traffic between the cluster units. You can adjust the distribution at any time. For example, if a low volume VDOM becomes a high volume VDOM you can move it from one cluster unit to another until the best balance is achieved. From the web-based manager you configure VDOM partitioning by setting the HA mode to active-passive and distributing virtual domains between Virtual Cluster 1 and Virtual Cluster 2. You can also configure different device priorities, port monitoring, and remote link failover, for Virtual Cluster 1 and Virtual Cluster 2.

From the CLI you configure VDOM partitioning by setting the HA mode to a-p. Then you configure device priority, port monitoring, and remote link failover and specify the VDOMs to include in virtual cluster 1. You do the same for virtual cluster 2 by entering the config secondary-vcluster command.

Failover protection does not change. If one cluster unit fails, all sessions are processed by the remaining cluster unit. No traffic interruption occurs for the virtual domains for which the still functioning cluster unit was the primary unit. Traffic may be interrupted temporarily for virtual domains for which the failed unit was the primary unit while processing fails over to the still functioning cluster unit. If the failed cluster unit restarts and rejoins the virtual cluster, VDOM partitioning load balancing is restored.

Example of inter-VDOM routing

This example shows how to configure a FortiGate unit to use inter-VDOM routing.

This section contains the follow topics:

- Network topology and assumptions
- Creating the VDOMs
- Configuring the physical interfaces
- Configuring the VDOM links
- Configuring the firewall and Security Profile settings
- Testing the configuration

Network topology and assumptions

Two departments of a company, Accounting and Sales, are connected to one FortiGate-800 unit. To do its work, the Sales department receives a lot of email from advertising companies that would appear to be spam if the Accounting department received it. For this reason, each department has its own VDOM to keep firewall policies and other configurations separate. A management VDOM makes sense to ensure company policies are followed for traffic content.

The traffic between Accounting and Sales will be email and HTTPS only. It could use a VDOM link for a meshed configuration, but we will keep from getting too complex. With the configuration, inter-VDOM traffic will have a slightly longer path to follow than normal—from one department VDOM, through the management VDOM, and back to the other department VDOM. Since inter-VDOM links are faster than physical interfaces, this longer path should not be noticed.

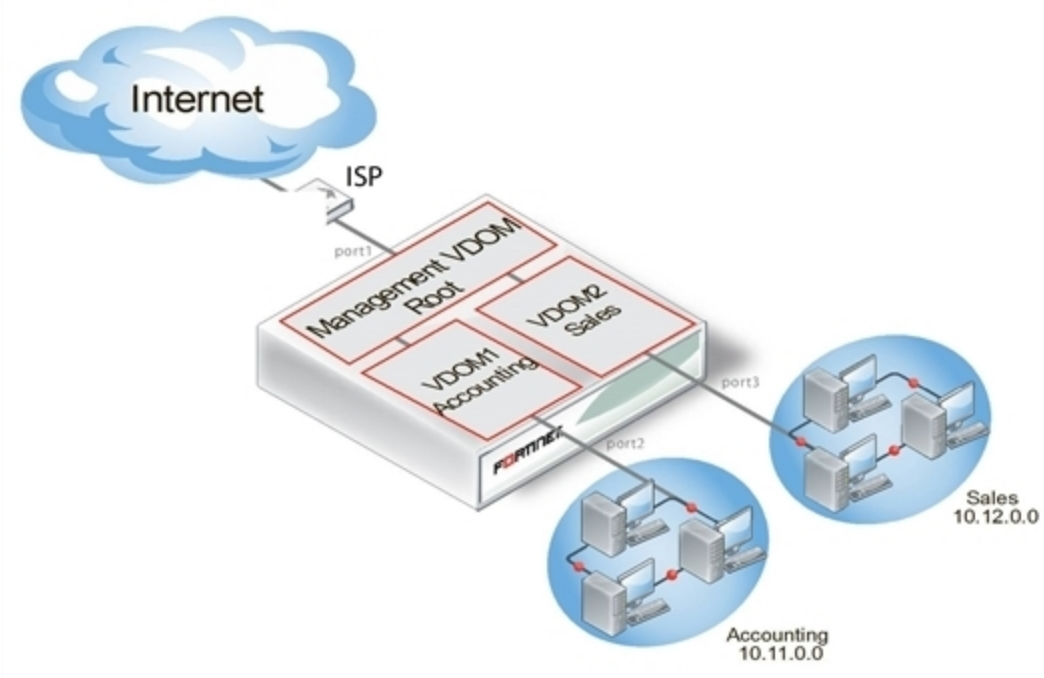
Firewall policies will be in place. For added security, firewall policies will allow only valid office services such as email, web browsing, and FTP between either department and the Internet. Any additional services that are required can be added in the future.

The company uses a single ISP to connect to the Internet. The ISP uses DHCP to provide an IP address to the FortiGate unit. Both departments use the same ISP to reach the Internet.

Other assumptions for this example are as follows:

- Your FortiGate unit has interfaces labelled port1 through port4 and VDOMs are not enabled.
- You are using the super_admin account.
- You have the FortiClient application installed.
- You are familiar with configuring interfaces, firewalls, and other common features on your FortiGate unit.

Management VDOM for two departments



General configuration steps

This example includes the following general steps. For best results, follow the steps in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the physical interfaces
3. Configuring the VDOM links
4. Configuring the firewall and Security Profile settings
5. Testing the configuration

Creating the VDOMs

This procedure enables VDOMs and creates the Sales and Accounting VDOMs.

To create the VDOMs - web-based manager:

1. Log in as the super_admin administrator.
2. Go to **System > Dashboard > Status > System Information > Virtual Domain**, and select **Enable**.
3. Log in again.
4. Go to **System > VDOM > VDOM**.
5. Select **Create New**, enter `Accounting` for the VDOM Name, and select **OK**.
6. Select **Create New**, enter `Sales` for the VDOM Name, and select **OK**.

To create the VDOMs - CLI:

```
config system global
   set vdom enable
end
config system vdom
   edit Accounting
   next
   edit Sales
   next
end
```

Configuring the physical interfaces

Next, the physical interfaces must be configured. This example uses three interfaces on the FortiGate unit - port2 (internal), port3(dmz), and port1(external). port2 and port3 interfaces each have a department's network connected. port1 is for all traffic to or from the Internet and will use DHCP to configure its IP address, which is common with many ISPs.

To configure the physical interfaces - web-based manager:

1. Go to **Global > Network** > Interfaces.
2. Select **Edit** for the port2 interface, enter the following information, and select **OK.**

Alias	AccountingLocal

Virtual Domain	Accounting
Addressing mode	Manual
IP/Netmask	172.100.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the accounting department internal interface.

3. Select **Edit** for the port3 interface, enter the following information, and select **OK**.

Alias	SalesLocal
Virtual Domain	Sales
Addressing mode	Manual
IP/Netmask	192.168.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the sales department internal interface.

4. Select **Edit** for the port1 interface, enter the following information, and select **OK**.

Alias	ManagementExternal
Virtual Domain	root
Addressing Mode	DHCP
Distance	5
Retrieve default gateway from server	Enable
Override internal DNS	Enable
Administrative Access	HTTPS, SSH, SNMP
Description	This is the accounting department internal interface.

When the mode is set to DHCP or PPoE on an interface you can set the distance field. This is the administrative distance for any routes learned through the gateway for this interface. The gateway is added to the static route table with these values. A lower distance indicates a preferred route.

To configure the physical interfaces - CLI:

```
config global
   config system interface
      edit port2
         set alias AccountingLocal
```

```
    set vdom Accounting
    set mode static
    set ip 172.100.1.1 255.255.0.0
    set allowaccess https ping ssh
    set description "The accounting dept internal interface"
next
edit port3
    set alias SalesLocal
    set vdom Sales
    set mode static
    set ip 192.168.1.1 255.255.0.0
    set allowaccess https ping ssh
    set description "The sales dept. internal interface"
next
edit port1
    set alias ManagementExternal
    set vdom root
    set mode DHCP
    set distance 5
    set gwdetect enable
    set dns-server-override enable
    set allowaccess https ssh snmp
    set description "The systemwide management interface."
end
```

Configuring the VDOM links

To complete the connection between each VDOM and the management VDOM, you need to add the two VDOM links; one pair is the Accounting - management link and the other is for Sales - management link.

When configuring inter-VDOM links, you do not have to assign IP addresses to the links unless you are using advanced features such as dynamic routing that require them. Not assigning IP addresses results in faster configuration, and more available IP addresses on your networks.

If you require them, or if you simply want to assign IP addresses for clarity can do so.

To configure the Accounting and management VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select the expand arrow to select **Create New > VDOM link**.
3. Enter the following information, and select **OK**.

Name		AccountVlnk
Interface #0		
	Virtual Domain	Accounting
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Accounting VDOM side of the link.

Interface #1		
	Virtual Domain	root
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Management VDOM side of the link.

To configure the Accounting and management VDOM link - CLI:

```
config global
   config system vdom-link
      edit AccountVlnk
      next
   end
   config system interface
      edit AccountVlnk0
         set vdom Accounting
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Accounting side of the VDOM link"
      next
      edit AccountVlnk1
         set vdom root
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Management side of the VDOM link"
      end
```

To configure the Sales and management VDOM link - web-based manager:

1. Go to **Global > Network** > Interfaces.
2. Select the expand arrow and select **Create New > VDOM link**.
3. Enter the following information, and select **OK**.

Name		SalesVlnk
Interface #0		
	Virtual Domain	Sales
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Sales VDOM side of the link.
Interface #1		

Virtual Domain	root
IP/Netmask	0.0.0.0/0.0.0.0
Administrative Access	HTTPS, PING, SSH
Description	The Management VDOM side of the link.

To configure the Sales and management VDOM link - CLI:

```
config global
   config system vdom-link
      edit SalesVlnk
   end
   config system interface
      edit SalesVlnk0
         set vdom Accounting
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Sales side of the VDOM link"
      next
      edit SalesVlnk1
         set vdom root
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Management side of the VDOM link"
      end
   end
```

Configuring the firewall and Security Profile settings

With the VDOMs, physical interfaces, and VDOM links configured the firewall must now be configured to allow the proper traffic. Firewalls are configured per-VDOM, and firewall objects must be created for each VDOM separately.

For this example, the firewall group of services allowed between the internal networks and the Internet are the basic services for web browsing, file transfer, and email. These include: HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, and SMTP.

The only services allowed between Sales and Accounting are secure web browsing (HTTPS) and email (POP3 and SMTP).

The limited number of services ensures security between departments. The list of services can be expanded in the future if needed.

Security profile settings will block all non-essential business websites while logging all web traffic, scan and file filter all web and email protocols, and block game and peer-to-peer applications using application control.

For added security, FortiClient is required on internal computers with AntiVirus scanning configured. This is enforced by **Endpoint NAC** in firewall policies.

Using firewall addresses makes the firewall policies easier to read. Also if any changes need to be made in the future, you can simply update the addresses without changing the firewall policies. The addresses required are:

- `AccountingLocal` - all traffic from the internal accounting network
- `AccountingVlnk` - all traffic from the VDOM link between accounting and management VDOMs
- `SalesLocal` - all traffic from the internal sales network
- `SalesVlnk` - all traffic from the VDOM link between sales and management VDOM.

The Accounting VDOM requires `AccountingLocal`, `AccountingVlnk`, and `SalesLocal`. The Sales VDOM requires `SalesLocal`, `SalesVlnk`, and `AccountingLocal`.

The firewall policies required on the Accounting VDOM are:

- AccountingLocal to Internet
- Internet to AccountingLocal
- SalesLocal to AccountingLocal
- AccountingLocal to SalesLocal

The firewall policies required on the Sales VDOM are:

- SalesLocal to Internet
- Internet to SalesLocal
- SalesLocal to AccountingLocal
- AccountingLocal to SalesLocal

This section includes the following topics:

- Configuring firewall service groups
- Configuring Security Profile settings for the Accounting VDOM
- Configuring firewall settings for the Accounting VDOM
- Configuring Security Profile settings for the Sales VDOM
- Configuring firewall settings for the Sales VDOM
- Configuring firewall settings between the Accounting and Sales VDOMs

Configuring firewall service groups

Service groups are an easy way to manage multiple services, especially if the same services are used on different networks.

The two service groups used here are intended for normal office traffic to the Internet, and for restricted traffic between departments. In both cases network traffic will be limited to the services listed to prevent any potential security risks or bandwidth-robbing applications.

These service groups can be changed as needed to either include additional valid services that are being used on the network, or to exclude services that are not required. Also, custom services can be created as needed for applications that are not listed.

To configure two firewall service groups - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Firewall Objects > Service > Group.**
3. Select **Create New**, enter the following information, and select **OK.**

Group Name	OfficeServices
Members	HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, PING, SMTP

4. Select **Create New**, enter the following information, and select **OK**.

Group Name	AccountingSalesServices
Members	HTTPS, POP3, PING, SMTP

To configure two firewall service groups - CLI:

```
config vdom
   edit Accounting
      config firewall service group
         edit OfficeServices
            set member HTTP HTTPS SSH FTP DNS NTP POP3 PING SMTP
         next
         edit AccountingSalesServices
            set member HTTPS POP3 PING SMTP
         end
   end
```

Configuring Security Profile settings for the Accounting VDOM

Security Profile settings include web filtering, antivirus, application control, and other features. This example just uses those three features to ensure that

- the business environment is free from viruses
- employees do not surf grossly inappropriate websites, and
- employees do not use games or peer-to-peer applications at work.

To configure web filtering for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Web Filter > Profile**.
3. Select **Create New**.
4. Enter `webStrict` for the **Name**.
5. Select the arrow to expand the **FortiGuard Web Filtering** section.
6. Block all **Categories** except Business Oriented, Other, and Unrated.
7. Block all **Classifications** except Image Search..
8. Log all **Categories** and **Classifications**.
9. Select **OK**.

To configure AntiVirus for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > AntiVirus > Profile**.
3. Select **Create New**.
4. Enter `avStrict` for the **Name**.

5. Enable **Scan** for all protocols.
6. Enable **File filter** for all protocols, and select `built-in-patterns` for **Option**.
7. Enable logging for both **Scan** and **File Filter**.
8. Select **OK**.

To configure application control for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Application Control > Application Sensor.**
3. Select **Create New** (+ button at top right of page).
4. Enter `appStrict` for **Name** and select OK.
5. Select **Create New**.
6. In **Filters**, set **Category** to **game**.
7. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

8. Select **Create New**.
9. In **Filters**, set **Category** to **p2p**.
10. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

11. Select **Apply**.

To configure application control for the Accounting VDOM - CLI:

```
config vdom
   edit Accounting
      config application list
         edit appStrict
            config entries
               edit 1
                  set category 2
               next
               edit 2
                  set category 8
               end
         end
   end
```

Configuring firewall settings for the Accounting VDOM

This configuration includes two firewall addresses and two firewall policies for the Accounting VDOM - one for the internal network, and one for the VDOM link with the management VDOM (root).

For added security, all traffic allowed will be scanned. Only valid office traffic will be allowed using the service group `OfficeServices`. The FortiClient application must be used to ensure additional protection for the sensitive accounting information.

All sales and accounting computers have the FortiClient application installed, so the firewall policies check that FortiClient is installed and that antivirus scanning is enabled.

Note the spelling of `AccountVlnk` which is due to the eleven character limit on VDOM link names.

To configure firewall addresses - web-based manager:

1. Open the **Accounting** VDOM.
2. Select **Firewall Objects > Address > Address**
3. Select **Create New**, enter the following information, and select **OK**.

Address Name	AccountingLocal
Type	Subnet/ IP Range
Subnet / IP Range	172.100.0.0
Interface	port1

4. Select **Create New**, enter the following information, and select **OK**.

Address Name	AccountManagement
Type	Subnet/ IP Range
Subnet / IP Range	10.0.1.0
Interface	AccountVlnk

To configure firewall addresses - CLI:

```
config vdom
   edit Accounting
      config firewall address
         edit AccountingLocal
            set type iprange
            set subnet 172.100.0.0
            set associated-interface port1
         next
         edit AccountManagement
            set type iprange
            set subnet 10.0.1.0
            set associated-interface AccountVlnk
         end
      end
```

To configure protocol options for Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Select **Policy > Policy > Protocol Options.**

3. Select **Create New**.
4. Enter `default` for the **Name**.
5. Select **OK**.

To configure the firewall policies from AccountingLocal to the Internet - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Policy > Policy**.
3. Select **Create New**, enter the following information, and then select **OK**.

Source Interface/Zone		port2
Source Address		AccountingLocal
Destination Interface/Zone		AccountVlnk
Destination Address		AccountManagement
Schedule		always
Service		OfficeServices
Action		ACCEPT
Enable NAT		enable
Security Features		enabled
	Protocol Option	default
	Web Filtering	webStrict
	AntiVirus Filtering	avStrict
	Application Control	appStrict
Enable Endpoint NAC		Enforce_FortiClient_AV

4. Open the **root** VDOM.
5. Go to **Policy > Policy.**
6. Select **Create New**, enter the following information, and then select **OK**.

Source Interface/Zone	AccountVlnk
Source Address	AccountManagement
Destination Interface/Zone	port2
Destination Address	all

Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Protocol Option	default
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict
Enable Endpoint NAC	disabled

To configure the firewall policies from AccountingLocal to Internet - CLI:

```
config vdom
   edit Accounting
      config firewall policy
         edit 1
            set srcintf "port2"
            set dstintf "AccountVlnk"
            set srcaddr "AccountingLocal"
            set dstaddr "AccountManagement"
            set action accept
            set schedule "always"
            set service "OfficeServices"
            set nat enable
            set av-profile avStrict
            set webfilter-profile webStrict
            set application-list appStrict
            set profile-protocol-options default
            set endpoint-check enable
            set endpoint-profile "FortiClient_installed"
         end
   end
config vdom
   edit root
      config firewall policy
         edit 2
            set srcintf AccountVlnk
            set dstintf port1
            set srcaddr AccountManagement
            set dstaddr all
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
            set av-profile "scan"
```

```
            set webfilter-profile "scan"
            set application-list "AppControlList"
            set profile-protocol-options default
            set endpoint-check disable
        end
    end
```

To configure the firewall policies from Internet to AccountingLocal - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy > Policy**.
3. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	port1
Source Address	all
Destination Interface/Zone	AccountVlnk
Destination Address	AccountManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Protocol Option	default
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict
Enable Endpoint NAC	disabled

4. Open the **Accounting** VDOM.
5. Go to **Policy > Policy.**
6. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	AccountVlnk
Source Address	AccountManagement
Destination Interface/Zone	port2

Destination Address	AccountingLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Protocol Option	default
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict
Enable Endpoint NAC	disabled

To configure the firewall policies from Internet to AccountingLocal - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 3
            set srcintf port1
            set dstintf AccountVlnk
            set srcaddr all
            set dstaddr AccountManagement
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
            set av-profile avStrict
            set webfilter-profile webStrict
            set application-list appstrict
            set profile-protocol-options default
            set endpoint-check disable
         end
   end
config vdom
   edit Accounting
      config firewall policy
         edit 4
            set srcintf AccountVlnk
            set dstintf port2
            set srcaddr AccountManagement
            set dstaddr AccountingLocal
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
```

```
            set av-profile avStrict
            set webfilter-profile webStrict
            set application-list appstrict
            set profile-protocol-options default
            set endpoint-check disable
        end
    end
```

Configuring Security Profile settings for the Sales VDOM

Security profile settings include web filtering, antivirus, application control, and other features. This example just uses those three features to ensure that

- the business environment is free from viruses
- employees do not surf grossly inappropriate websites, and
- employees do not use games or peer-to-peer applications at work.

Note that Sales web traffic is different from Accounting, and web filtering is different to account for this.

To configure web filtering for the Sales VDOM - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Security Profiles > Web Filter > Profile**.
3. Select **Create New**.
4. Enter `webStrict` for the **Name**.
5. In **FortiGuard Categories**, select all of the categories except **Bandwidth Consuming**, **General Interest - Business** and **Unrated**.
6. In **Change Action for Selected Categories** select **Block**.
7. Select **Apply**.

To configure web filtering for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config webfilter profile
         edit webStrict
            config ftgd-wf
               set allow g07 g08 g21 g22 c01 c03
               set deny g01 g02 g03 g04 g05 g06 c02 c04 c05 c06 c07
            end
            set web-ftgd-err-log enable
         end
   end
```

To configure AntiVirus for the Sales VDOM - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Security Profiles > AntiVirus > Profile**.
3. Select **Create New**.
4. Enter `avStrict` for the **Name**.
5. Enable virus scan for all protocols.
6. Select **Apply**.

To configure AntiVirus for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config antivirus profile
         edit "avStrict"
            config http
               set options scan file-filter
            end
            config ftp
               set options scan file-filter
            end
            config imap
               set options scan file-filter
            end
            config pop3
               set options scan file-filter
            end
            config smtp
               set options scan file-filter
            end
            config nntp
               set options scan file-filter
            end
            config im
               set options scan file-filter
            end
            set filepattable 1
            set av-virus-log enable
            set av-block-log enable
         end
   end
```

To configure application control for the Sales VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Application Control > Application Sensor.**
3. Select **Create New** (+ button at top right of page).
4. Enter `appStrict` for **Name** and select OK.
5. Select **Create New**.
6. In **Filters**, set **Category** to **game**.
7. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

8. Select **Create New**.
9. In **Filters**, set **Category** to **p2p**.
10. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

11. Select **Apply**.

To configure application control for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config application list
         edit "appStrict"
            config entries
               edit 1
                  set category 2
               next
               edit 2
                  set category 8
               end
         end
   end
```

Configuring firewall settings for the Sales VDOM

Like the Accounting firewall settings, this configuration includes two firewall addresses and two firewall policies for the sales VDOM: one for the internal network, and one for the VDOM link with the management VDOM.

When entering the CLI commands, the number of the firewall policies must be high enough to be a new policy. Depending on the number of firewall policies on your FortiGate unit, this may require starting at a higher number than the 6 required for the default configuration. This number is added automatically when you configure firewall policies using the web manager interface.

The FortiClient application must be used on Sales network computers to ensure additional protection for the sensitive information and for protection against spam.

To configure firewall addresses - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Firewall Objects > Address > Address.**
3. Select **Create New,** enter the following information, and select **OK**.

Address Name	SalesLocal
Type	Subnet / IP Range
Subnet / IP Range	172.100.0.0
Interface	port3

4. Go to **Firewall Objects > Addresses.**
5. Select **Create New**, enter the following information, and select **OK**.

Address Name	SalesManagement
Type	Subnet / IP Range
Subnet / IP Range	10.0.1.0
Interface	SalesVlnk

To configure the firewall addresses - CLI:

```
config vdom
   edit Sales
      config fireall address
         edit SalesLocal
            set type iprange
            set subnet 172.100.0.0
            set associated-interface port2
         next
         edit SalesManagement
            set type iprange
            set subnet 10.0.1.0
            set associated-interface SalesVlnk
         end
   end
```

To configure the firewall policies from SalesLocal to the Internet - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Policy > Policy.**
3. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	port3
Source Address	SalesLocal
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

4. Open the **root** VDOM.
5. Go to **Policy > Policy.**

6. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	external
Destination Address	all
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

To configure the firewall policies from SalesLocal to the Internet - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 6
            set srcintf port2
            set srcaddr SalesLocal
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service OfficeServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
            set endpoint-check enable
            set endpoint-redir-portal enable
         end
   end
config vdom
   edit Sales
      config firewall policy
         edit 7
            set srcintf SalesVlnk
            set srcaddr SalesManagement
            set dstintf external
            set dstaddr all
            set schedule always
            set service OfficeServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
```

```
            set endpoint-check enable
        end
    end
```

To configure the firewall policies from the Internet to SalesLocal - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy > Policy.**
3. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	external
Source Address	all
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

4. Open the **Sales** VDOM.
5. Go to **Policy > Policy.**
6. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	port2
Destination Address	SalesLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled

Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

To configure the firewall policies from the Internet to SalesLocal - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 8
            set srcintf external
            set srcaddr all
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service OfficeServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
            set endpoint-check enable
            set endpoint-redir-portal enable
         end
   end
config vdom
   edit Sales
      config firewall policy
         edit 9
            set srcintf SalesVlnk
            set srcaddr SalesManagement
            set dstintf port2
            set dstaddr SalesLocal
            set schedule always
            set service OfficeServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
            set endpoint-check enable
            set endpoint-redir-portal enable
         end
   end
```

Configuring firewall settings between the Accounting and Sales VDOMs

Firewall policies are required for any communication between each internal network and the Internet. Policies are also required for the two internal networks to communicate with each other through the management VDOM.

The more limited AccountingSalesServices group of services will be used between Sales and Accounting to ensure the traffic is necessary business traffic only. These policies will result in a partially meshed VDOM configuration. The FortiClient application must be used to ensure additional protection for the sensitive accounting information.

Two firewall policies are required to allow traffic in both directions between Sales and Accounting.

To configure the firewall policy between Sales and Accounting on the management VDOM - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy > Policy.**
3. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	AccountVlnk
Destination Address	AccountingManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

4. Go to **Policy > Policy.**
5. Select **Create New**, enter the following information, and select **OK**.

Source Interface/Zone	AccountVlnk
Source Address	AccountingManagement
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled

Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

To configure the firewall policy between Sales and Accounting on the management VDOM - CLI:

```
config vdom
   edit root
      config system firewall policy
         edit 9
            set srcintf SalesVlnk
            set srcaddr SalesManagement
            set dstintf AccountVlnk
            set dstaddr AccountManagement
            set schedule always
            set service AccountingSalesServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
            set endpoint-check enable
            set endpoint-redir-portal enable
         next
         edit 10
            set srcintf AccountVlnk
            set srcaddr AccountManagement
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service AccountingSalesServices
            set action accept
            set profile-status enable
            set profile scan
            set logtraffic enable
            set endpoint-check enable
            set endpoint-redir-portal enable
         end
   end
```

Testing the configuration

Once the inter-VDOM routing has been configured, tests must be conducted to confirm proper operation. If there are any problems, use the troubleshooting tips to resolve them.

This section includes the following topics:

- Testing connectivity
- Troubleshooting Tips

Testing connectivity

Testing connectivity ensures that physical networking connections as well as FortiGate unit interface configurations, including firewall policies, are properly configured.

The easiest way to test connectivity is to use the `ping` and `traceroute` commands to confirm the connectivity of different routes on the network. Include testing:

- from AccountingLocal to Internet
- from Internet to AccountingLocal
- from SalesLocal to Internet
- from Internet to SalesLocal
- from AccountingLocal to SalesLocal.

When using the commands on a Windows computer, go to a command line prompt and enter either `ping <IP address>` or `tracert <IP address>`.

When using the commands on a FortiGate unit, go to the CLI and enter either `exec ping <IP address>` or `exec traceroute <IP address>`.

Troubleshooting Tips

When there are problems with connectivity, the following troubleshooting tips will help resolve the issues.

- If a multiple hop test, such as traceroute, is not successful then reduce it to a single hop to simplify the test. Test each link of the path to see which hop is down. If all hops are up, check the FortiGate unit policies to ensure they allow basic traffic to flow as expected.
- If ping does not work, confirm that the FortiGate unit interfaces have Ping enabled and also ensure Ping is enabled in the firewall policies. Otherwise the Ping traffic will be blocked.
- If one protocol does not work but others do work, check the FortiGate unit firewall policies for that one protocol to ensure it is allowed.
- If there are unexplained connectivity problems, check the local computer to ensure it does not have a software firewall running that may be blocking traffic. MS Windows computers have a firewall running by default that can cause problems.

For additional troubleshooting, see Troubleshooting Virtual Domains.

Troubleshooting Virtual Domains

When you are configuring VDOMs you may run into some issues, with your VDOM configuration, your network configuration, or your device setup. This section addresses common problems and specific concerns that an administrator of a VDOM network may have.

This section includes:

- VDOM admin having problems gaining access
- FortiGate unit running very slowly
- General VDOM tips and troubleshooting

VDOM admin having problems gaining access

With VDOMs configured, administrators have an extra layer of permissions and may have problems accessing their information.

Confirm the admin's VDOM

Each administrator account, other than the super_admin account, is tied to one specific VDOM. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM.

Confirm the VDOM's interfaces

An administrator can only access their VDOM through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable there will be no method of accessing that VDOM by its local administrator. The super_admin will be required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.

Confirm the VDOMs admin access

As with all FortiGate units, administration access on the VDOM's interfaces must be enabled for that VDOM's administrators to gain access. For example if SSH is not enabled, that is not available to administrators.

To enable admin access, the super_admin will go to the **Global > Network > Interfaces** page, and for the interface in question enable the admin access.

FortiGate unit running very slowly

You may experience a number of problems resulting from your FortiGate unit being overloaded. These problems may appear as:

- CPU and memory threshold limits exceeded on a continual basis
- AV failopen happening on a regular basis
- dropped traffic or sessions due to lack of resources

These problems are caused by a lack of system resources. There are a number of possible reasons for this.

Too many VDOMs

If you have configured many VDOMs on your system, past the default ten VDOMs, this could easily be your problem.

Each VDOM you create on your FortiGate unit requires system resources to function - CPU cycles, memory, and disk space. When there are too many VDOMs configured there are not enough resources for operation. This may be a lack of memory in the session table, or no CPU cycles for processing incoming IPS traffic, or even a full disk drive.

Go to **System > VDOM** and see the number of configured VDOMs on your system. If you are running 500 or more VDOMs, you must have a FortiGate 5000 chassis. Otherwise you need to reduce the number of VDOMs on your system to fix the problem. Even if you have the proper hardware, you may encounter noticeably slow throughput if you are using advanced features such as security profiles or deep content inspection with many configured VDOMs.

One or more VDOMs are consuming all the resources

If you have sufficient hardware to support the number of VDOMs you are running, check the global resources on your FortiGate unit. At a glance it will tell you if you are running out of a particular resource such as sessions, or users. If this is the case, you can then check your VDOMs to see if one particular VDOM is using more than its share of resources. If that is the case you can change the resource settings to allow that VDOM (or those VDOMs) fewer resources and in turn allow the other VDOMs access to those resources.

Too many Security Features in use

It is likely that reducing the Security Features in use regardless of number of VDOMs will greatly improve overall system performance and should be considered as an option.

Finally it is possible that your FortiGate unit configuration is incorrect in some other area, which is using up all your resources. For example, forgetting that you are running a network sniffer on an interface will create significant amounts of traffic that may prevent normal operation.

General VDOM tips and troubleshooting

Besides ping and traceroute, there are additional tools for troubleshooting your VDOM configurations. These include packet sniffing and debugging the packet flow.

Perform a sniffer trace

When troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the route you expect that they are. Packet sniffing can also be called a network tap, packet capture, or logic analyzing.

If your FortiGate unit has NP interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP interfaces, you should disable off-loading on those interfaces.

What sniffing packets can tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, what the port of entry is on the FortiGate unit, if the ARP resolution is correct, and if the traffic is being sent back to the source as expected.

Sniffing packets can also tell you if the Fortigate unit is silently dropping packets for reasons such as RPF (Reverse Path Forwarding), also called Anti Spoofing, which prevents an IP packet from being forwarded if its Source IP does not either belong to a locally attached subnet (local interface), or be part of the routing between the FortiGate and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymmetric enable`), however this will disable stateful inspection on the FortiGate unit and cause many features to be turned off.

If you configure virtual IP addresses on your Fortigate unit, it will use those addresses in preference to the physical IP addresses. You will notice this when you are sniffing packets because all the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

How to sniff packets

When you are using VDOMs, you must be in a VDOM to access the `diag sniffer` command. At the global level, the command is not available. This is limit the packets only to the ones on your VDOM, and protects the privacy of other VDOM clients.

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

<interface_name>	The name of the interface to sniff, such as “port1” or “internal”. This can also be “any” to sniff all interfaces.
<‘filter’>	What to look for in the information the sniffer reads. “none” indicates no filtering, and all packets will be displayed as the other arguments indicate. The filter must be inside single quotes (‘).
<verbose>	The level of verbosity as one of: **1 -** print header of packets **2 -** print header and data from IP of packets **3 -** print header and data from Ethernet of packets
<count>	The number of packets the sniffer reads before stopping. If you don’t put a number here, the sniffer will run forever unit you stop it with <CTRL C>.

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next 3 packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757

0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

For a more advanced example of packet sniffing, the following commands will report packets on any interface travelling between a computer with the host name of `PC1` and the computer with the host name of `PC2`. With verbosity 4 and above, the sniffer trace will display the interface names where traffic enters or leaves the FortiGate unit. Remember to stop the sniffer, type `CTRL+C`. Note that `PC1` and `PC2` may be VDOMs.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2>" 4
```

or

```
FGT# diagnose sniffer packet any "(host <PC1> or host <PC2>) and icmp" 4
```

The following sniffer CLI command includes the ARP protocol in the filter which may be useful to troubleshoot a failure in the ARP resolution (for instance PC2 may be down and not responding to the FortiGate ARP requests).

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4
```

Debugging the packet flow

Traffic should come in and leave the VDOM. If you have determined that network traffic is not entering and leaving the VDOM as expected, debug the packet flow.

Debugging can only be performed using CLI commands. Debugging the packet flow requires a number of debug commands to be entered as each one configures part of the debug action, with the final command starting the debug.

If your FortiGate unit has NP interfaces that are offloading traffic, this will change the packet flow. Before performing the debug on any NP interfaces, you should disable offloading on those interfaces.

The following configuration assumes that `PC1` is connected to the internal interface of the FortiGate unit and has an IP address of `10.11.101.200`. `PC1` is the host name of the computer.

To debug the packet flow in the CLI, enter the following commands:

```
FGT# diag debug enable
FGT# diag debug flow filter add <PC1>
FGT# diag debug flow show console enable
FGT# diag debug flow trace start 100
FGT# diag debug enable
```

The `start 100` argument in the above list of commands will limit the output to 100 packets from the flow. This is useful for looking at the flow without flooding your log or your display with too much information.

To stop all other debug activities, enter the command:

```
FGT# diag debug flow trace stop
```

The following is an example of debug flow output for traffic that has no matching Firewall Policy, and is in turn blocked by the FortiGate unit. The denied message indicates the traffic was blocked. Note that even with VDOMs not enabled, vd-root is still shown.

```
id=20085 trace_id=319 func=resolve_ip_tuple_fast line=2825 msg="vd-root received a
    packet(proto=6, 192.168.129.136:2854->192.168.96.153:1863) from port3."

id=20085 trace_id=319 func=resolve_ip_tuple line=2924 msg="allocate a new session-
    013004ac"

id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a route: gw-
    192.168.150.129 via port1"

id=20085 trace_id=319 func=fw_forward_handler line=248 msg=" Denied by forward policy
    check"
```

Chapter 28 - VM Installation

This document describes how to deploy a FortiGate virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For these issues, see the FortiGate 5.2 Handbook.

This document includes the following sections:

- FortiGate VM Overview
- Deployment example – VMware
- Deployment example – MS Hyper-V
- Deployment example – KVM
- Deployment example – OpenXen
- Deployment example – Citrix XenServer

FortiGate VM Overview

The following topics are included in this section:

FortiGate VM models and licensing
Registering FortiGate VM with Customer Service & Support
Downloading the FortiGate VM deployment package
Deployment package contents
Deploying the FortiGate VM appliance

FortiGate VM models and licensing

Fortinet offers the FortiGate VM in five virtual appliance models determined by license. When configuring your FortiGate VM, be sure to configure hardware settings within the ranges outlined below. Contact your Fortinet Authorized Reseller for more information.

FortiGate VM model information

Technical Specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08
Virtual CPUs (min / max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Virtual Network Interfaces (min / max)			2 / 10		
Virtual Memory (min / max)	1GB / 1GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB /12GB
Virtual Storage (min / max)			32GB / 2TB		
Managed Wireless APs (tunnel mode / global)	32 / 32	32 / 64	256 / 512	256 / 512	1024 / 4096
Virtual Domains (default / max)	1 / 1	10 / 10	10 / 25	10 / 50	10 / 250

After placing an order for FortiGate VM, a license registration code is sent to the email address used on the order form. Use the registration number provided to register the FortiGate VM with Customer Service & Support and then download the license file. Once the license file is uploaded to the FortiGate VM and validated, your FortiGate VM appliance is fully functional.

FortiGate VM evaluation license

FortiGate VM includes a limited embedded 15-day trial license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- low encryption only (no HTTPS administrative access)
- all features except FortiGuard updates

You cannot upgrade the firmware, doing so will lock the Web-based Manager until a license is uploaded. Technical support is not included. The trial period begins the first time you start FortiGate VM. After the trial license expires, functionality is disabled until you upload a license file.

Registering FortiGate VM with Customer Service & Support

To obtain the FortiGate VM license file you must first register your FortiGate VM with Customer Service & Support.

To register your FortiGate VM:

1. Log in to the Customer Service & Support portal using an existing support account or select **Sign Up** to create a new account.
2. In the main page, under **Asset**, select **Register/Renew**.

   The **Registration** page opens.
3. Enter the registration code that was emailed to you and select **Register**. A registration form will display.
4. After completing the form, a registration acknowledgement page will appear.
5. Select the **License File Download** link.
6. You will be prompted to save the license file (`.lic`) to your local computer. See "Upload the license file" for instructions on uploading the license file to your FortiGate VM via the Web-based Manager.

Downloading the FortiGate VM deployment package

FortiGate VM deployment packages are included with FortiGate firmware images on the Customer Service & Support site. First, see the following table to determine the appropriate VM deployment package for your VM platform.

Selecting the correct FortiGate VM deployment package for your VM platform

VM Platform	FortiGate VM Deployment File
Citrix XenServer v5.6sp2, 6.0 and later	FGT_VM64-v500-buildnnnn-FORTINET.out.CitrixXen.zip
OpenXen v3.4.3, 4.1	FGT_VM64-v500-buildnnnn-FORTINET.out.OpenXen.zip
Microsoft Hyper-V Server 2008R2 and 2012	FGT_VM64-v500-buildnnnn-FORTINET.out.hyperv.zip
KVM (qemu 0.12.1)	FGT_VM64-v500-buildnnnn-FORTINET.out.kvm.zip
VMware ESX 4.0, 4.1 ESXi 4.0/4.1/5.0/5.1/5.5	FGT_VM32-v500-buildnnnn-FORTINET.out.ovf.zip (32-bit) FGT_VM64-v500-buildnnnn-FORTINET.out.ovf.zip

For more information see the FortiGate product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortigate/virtualappliances.html.

The firmware images FTP directory is organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FGT_VM32-v500-build0151-FORTINET.out.ovf.zip image found in the v5.0 Patch Release 2 directory is specific to the FortiGate VM 32-bit environment.

You can also download the FortiOS Release Notes, FORTINET-FORTIGATE MIB file, FSSO images, and SSL VPN client in this directory. The Fortinet Core MIB file is located in the main FortiGate v5.00 directory.

To download the FortiGate VM deployment package:

1. In the main page of the Customer Service & Support site, select **Download** > **Firmware Images**.

   The **Firmware Images** page opens.
2. In the **Firmware Images** page, select **FortiGate**.
3. Browse to the appropriate directory on the FTP site for the version that you would like to download.
4. Download the appropriate `.zip` file for your VM server platform.

   You can also download the FortiGate Release Notes.
5. Extract the contents of the deployment package to a new file folder.

Deployment package contents

Citrix XenServer

The FORTINET.out.CitrixXen.zip file contains:

- fortios.vhd: the FortiGate VM system hard disk in VHD format
- fortios.xva: binary file containing virtual hardware configuration settings
- in the ovf folder:
  - FortiGate-VM64.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen
  - fortios.vmdk: the FortiGate VM system hard disk in VMDK format
  - datadrive.vmdk: the FortiGate VM log disk in VMDK format

The ovf folder and its contents is an alternative method of installation to the .xva and VHD disk image.

OpenXEN

The FORTINET.out.OpenXen.zip file contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

Microsoft Hyper-V

The FORTINET.out.hyperv.zip file contains:

- in the Virtual Hard Disks folder:
  - fortios.vhd: the FortiGate VM system hard disk in VHD format
  - DATADRIVE.vhd: the FortiGate VM log disk in VHD format
- In the Virtual Machines folder:
  - fortios.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiGate VM state here

KVM

The FORTINET.out.kvm.zip contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

VMware ESX/ESXi

You will need to create a 32GB log disk.

The FORTINET.out.ovf.zip file contains:

- fortios.vmdk: the FortiGate VM system hard disk in VMDK format
- datadrive.vmdk: the FortiGate VM log disk in VMDK format
- Open Virtualization Format (OVF) template files:
  - FortiGate-VM64.ovf: OVF template based on Intel e1000 NIC driver
  - FortiGate-VM64.hw04.ovf: OVF template file for older (v3.5) VMware ESX server
  - FortiGate-VMxx.hw07_vmxnet2.ovf: OVF template file for VMware vmxnet2 driver
  - FortiGate-VMxx.hw07_vmxnet3.ovf: OVF template file for VMware vmxnet3 driver

Use the VMXNET3 interface (FortiGate-VMxx.hw07_vmxnet3.ovf template) if the virtual appliance will distribute workload to multiple processor cores.

Deploying the FortiGate VM appliance

Prior to deploying the FortiGate VM appliance, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiGate VM assume that

- You are familiar with the management software and terminology of your VM platform.
- An Internet connection is available for FortiGate VM to contact FortiGuard to validate its license or, for closed environments, a FortiManager can be contacted to validate the FortiGate VM license. See "Validate the FortiGate VM license with FortiManager".

For assistance in deploying FortiGate VM, refer to the deployment chapter in this guide that corresponds to your VMware environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiGate VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiGate VM, you will have access only through the console window of your VM server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate VM web-based manager.

After deployment and license validation, you can upgrade your FortiGate VM appliance's firmware by downloading either FGT_VM32-v500-buildnnnn-FORTINET.out (32-bit) or FGT_VM64-v500-buildnnnn-FORTINET.out (64-bit) firmware. Firmware upgrading on a VM is very similar to upgrading firmware on a hardware FortiGate unit.

Deployment example – VMware

Once you have downloaded the FGT_VMxx-v5-build0xxx-FORTINET.out.ovf.zip file from http://support.fortinet.com and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

The following topics are included in this section:

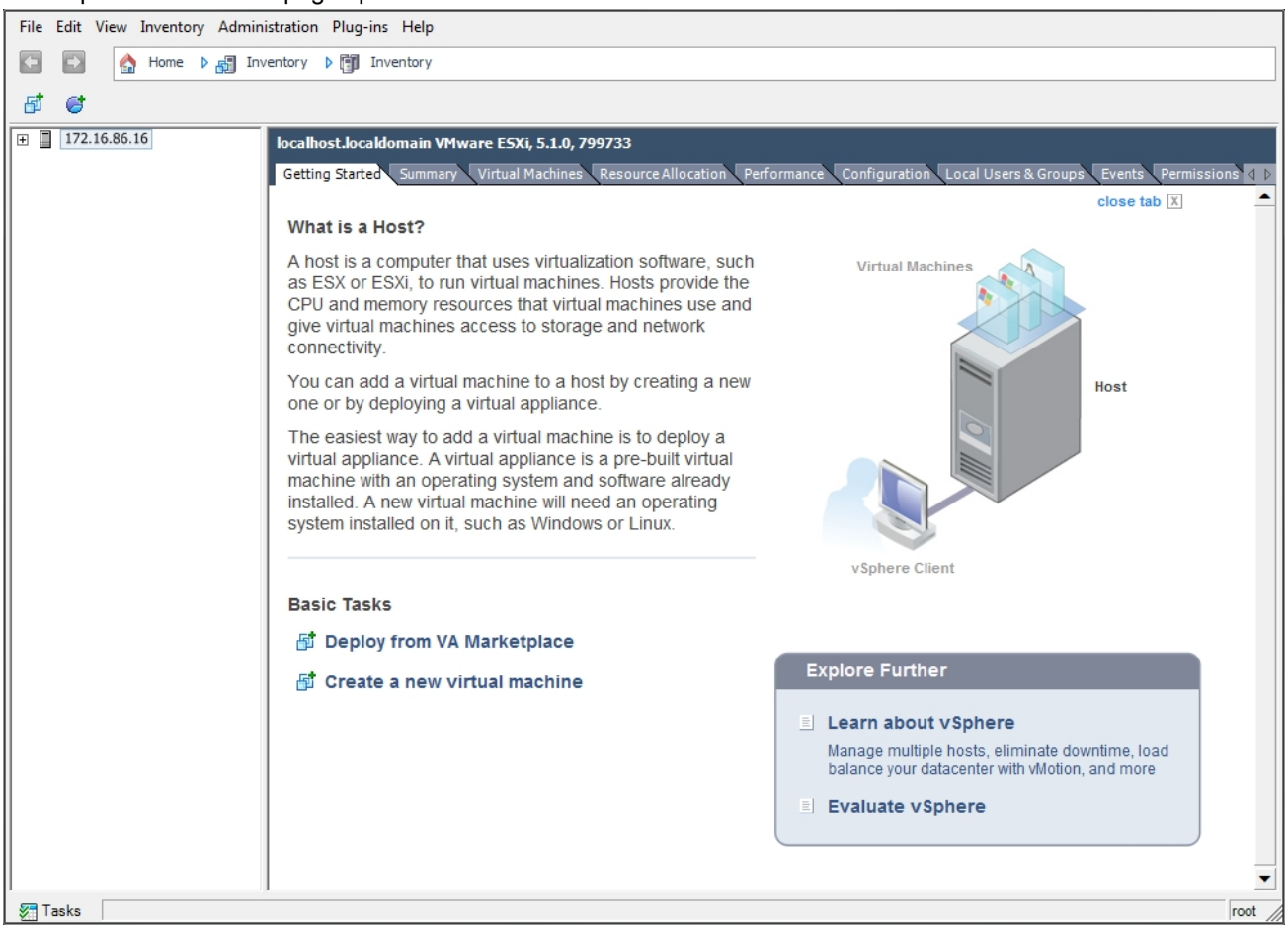
Open the FortiGate VM OVF file with the vSphere client
Configure FortiGate VM hardware settings
Transparent mode VMware configuration
High Availability VMware configuration
Power on your FortiGate VM

Open the FortiGate VM OVF file with the vSphere client

To deploy the FortiGate VM OVF template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password and select **Login**.

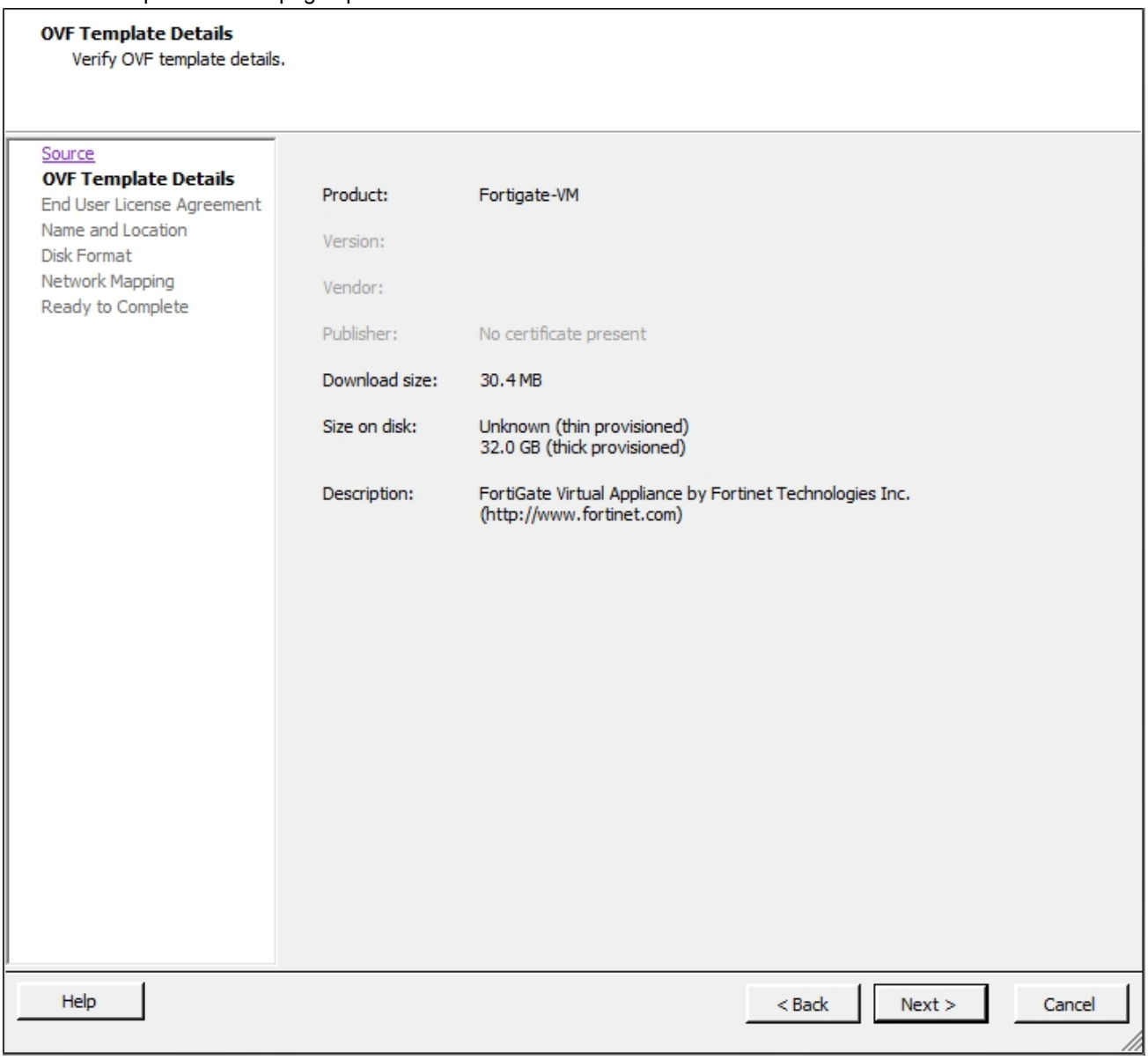
The vSphere client home page opens.



2. Select **File > Deploy OVF Template** to launch the OVF Template wizard.

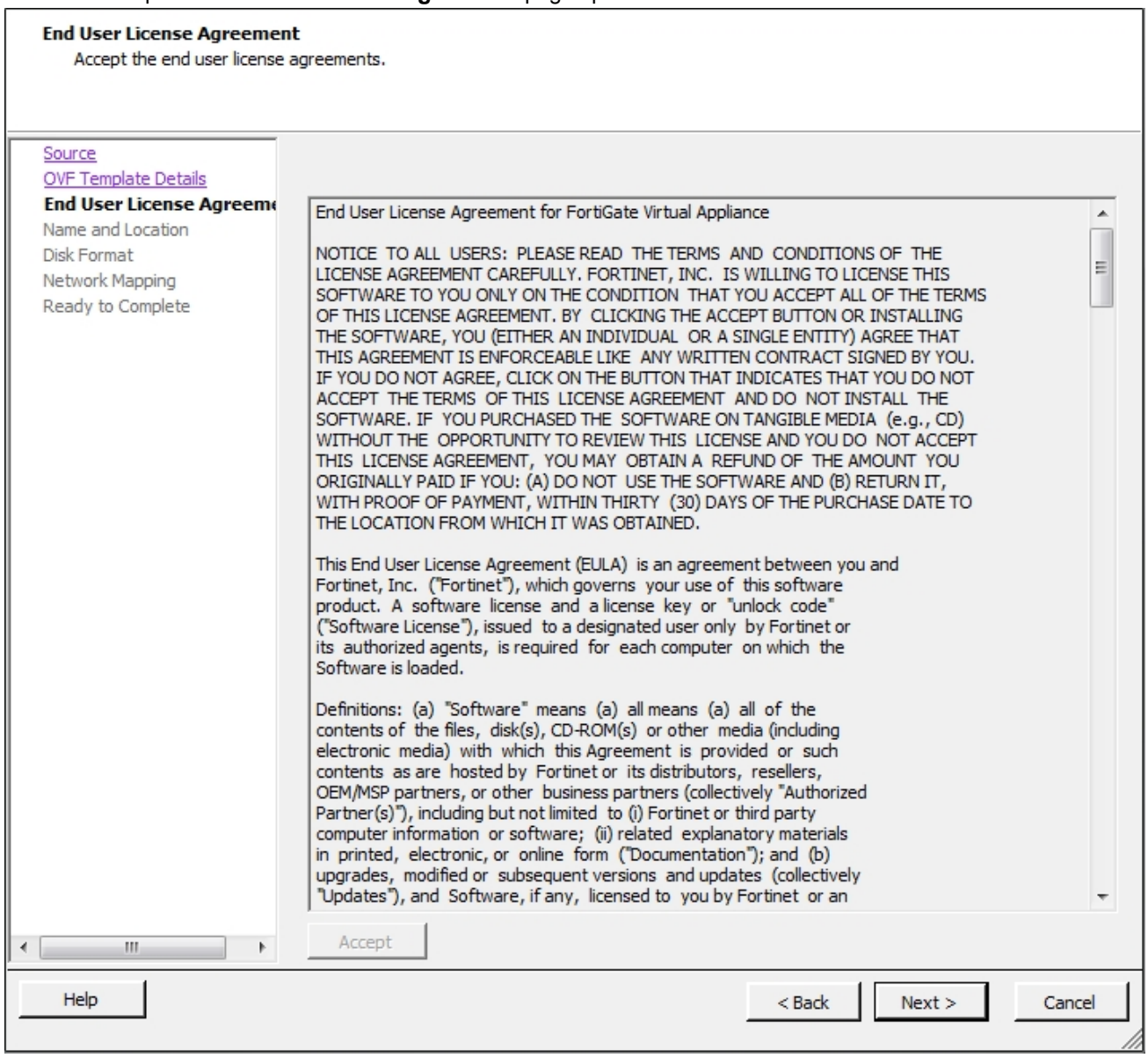
   The OVF Template **Source** page opens.
3. Select the source location of the OVF file. Select **Browse** and locate the OVF file on your computer. Select **Next** to continue.

The OVF Template **Details** page opens.



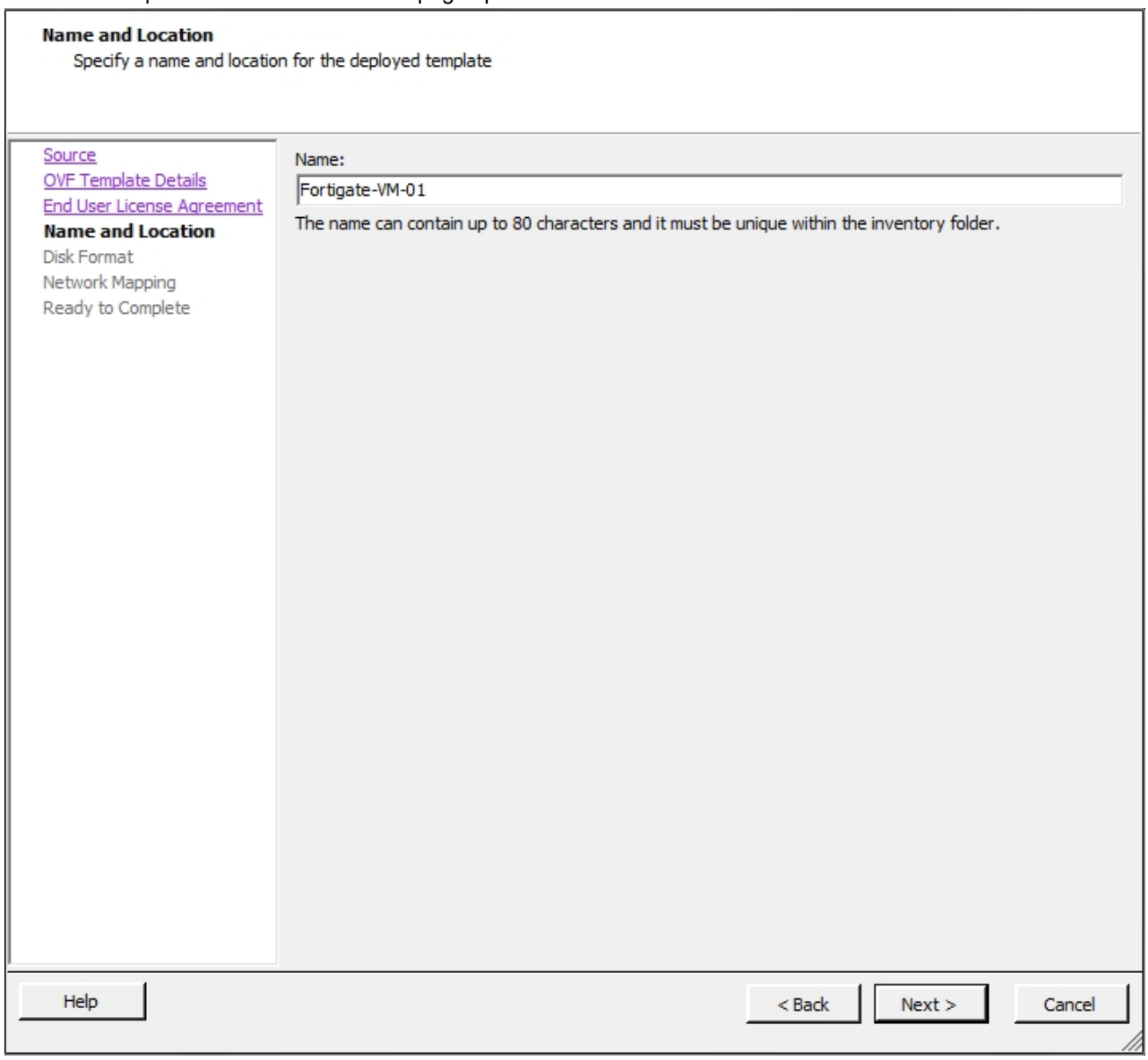
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select **Next** to continue.

The OVF Template **End User License Agreement** page opens.



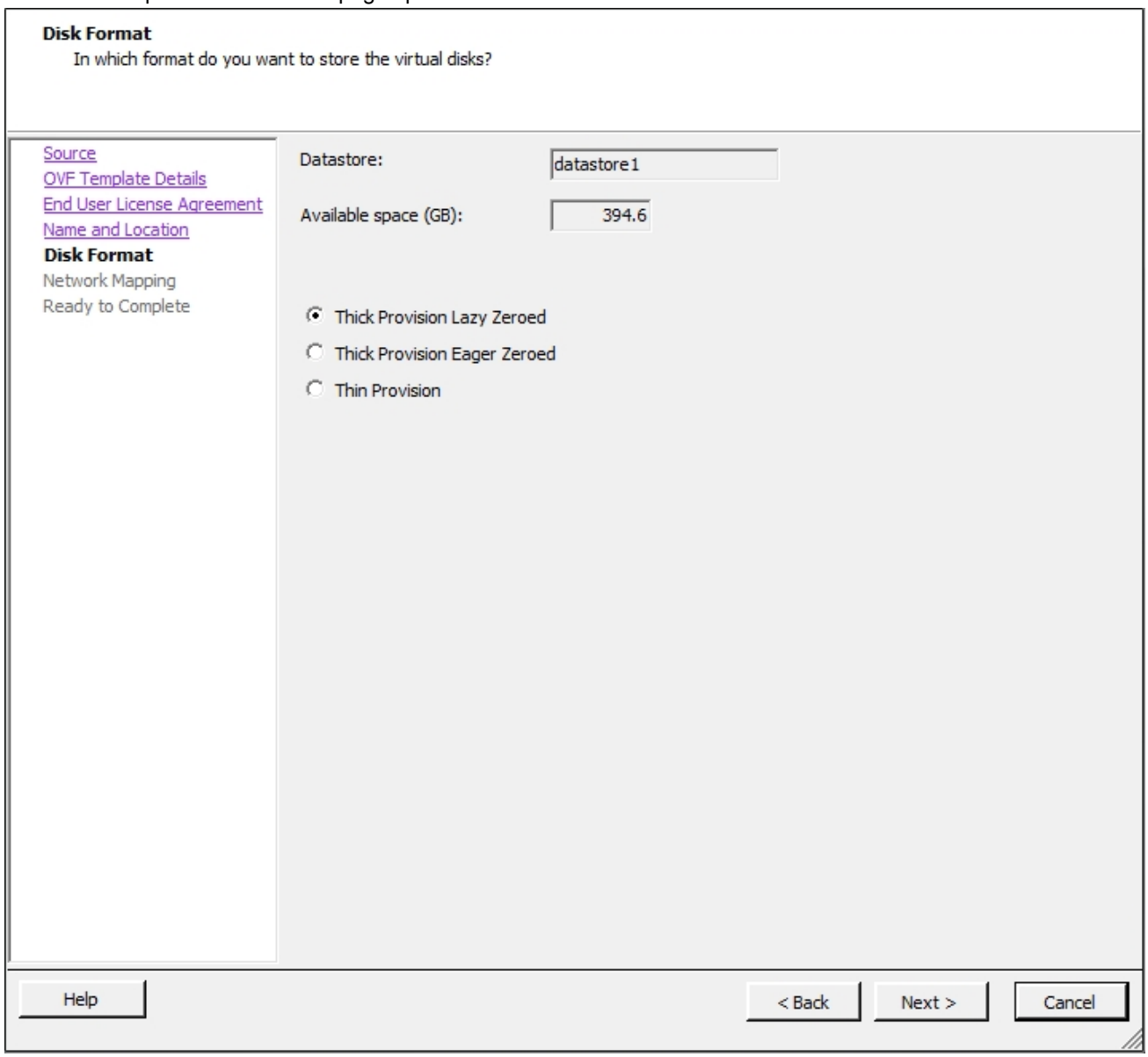
5. Read the end user license agreement for FortiGate VM. Select **Accept** and then select **Next** to continue.

The OVF Template **Name and Location** page opens.



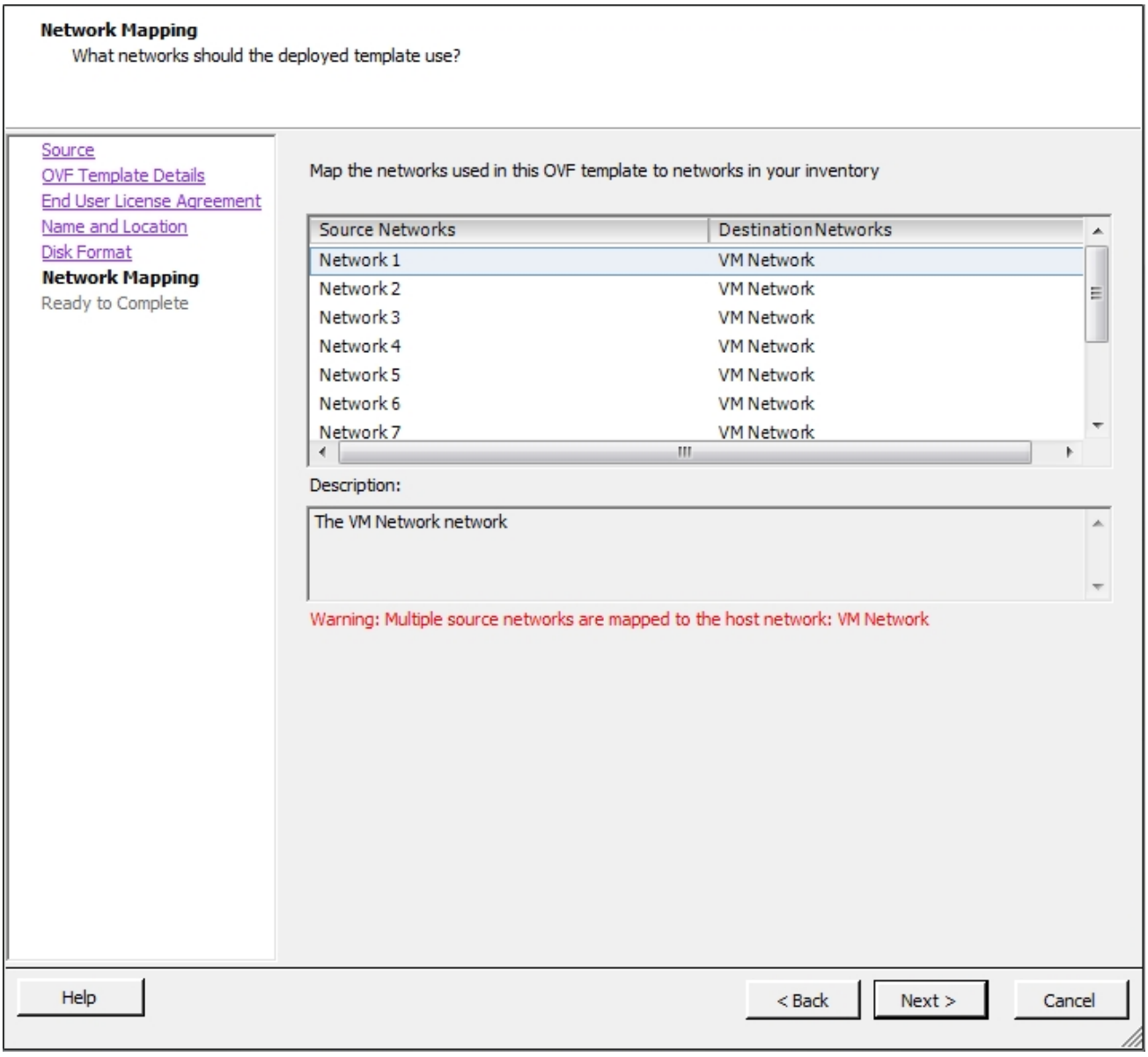
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select **Next** to continue.

The OVF Template **Disk Format** page opens.



7. Select one of the following:
   - **Thick Provision Lazy Zeroed**: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - **Thick Provision Eager Zeroed**: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - **Thin Provision**: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless if you have deleted data, etc.
8. Select **Next** to continue.

   The OVF Template **Network Mapping** page opens.

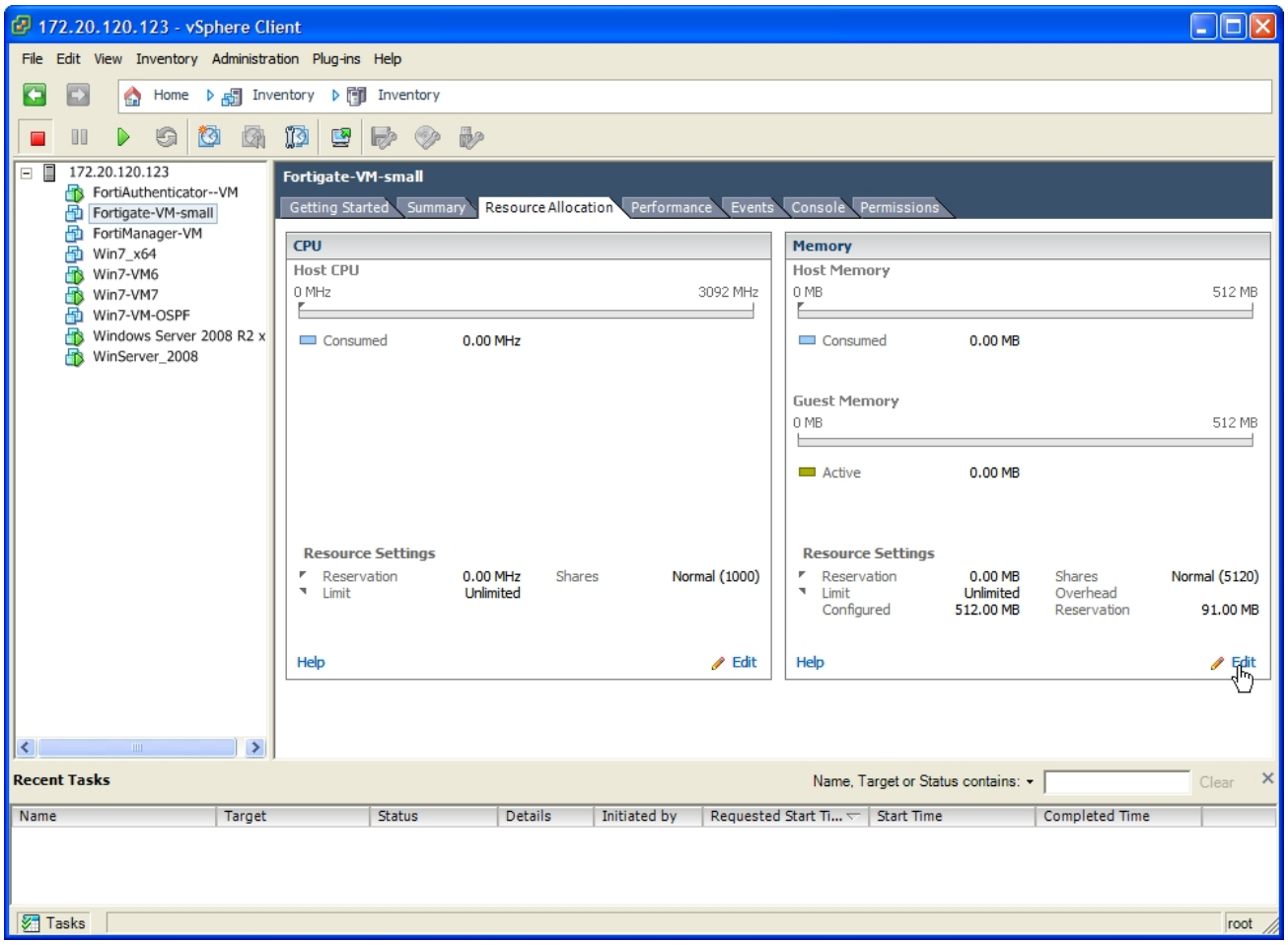


9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiGate VM. You must set the destination network for this entry to access the device console. Select **Next** to continue.

   The OVF Template **Ready to Complete** page opens.
10. Review the template configuration. Make sure that **Power on after deployment** is not enabled. You might need to configure the FortiGate VM hardware settings prior to powering on the FortiGate VM.
11. Select **Finish** to deploy the OVF template. You will receive a **Deployment Completed Successfully** dialog box once the FortiGate VM OVF template wizard has finished.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.



Transparent mode VMware configuration

If you want to use your FortiGate-VM in transparent mode, your VMware server's virtual switches must operate in promiscuous mode. This permits these interfaces to receive traffic that will pass through the FortiGate unit but was not addressed to the FortiGate unit.

In VMware, promiscuous mode must be explicitly enabled:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of vSwitch0.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.
7. Repeat steps 3 through 6 for other vSwitches that your transparent mode FortiGate-VM uses.

High Availability VMware configuration

If you want to combine two or more FortiGate-VM instances into a FortiGate Clustering Protocol (FGCP) High Availability (HA) cluster the VMware server's virtual switches used to connect the heartbeat interfaces must operate in promiscuous mode. This permits HA heartbeat communication between the heartbeat interfaces. HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. The FGCP uses link-local IP4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

To enable promiscuous mode in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect heartbeat interfaces.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.

You must also set the virtual switches connected to other FortiGate interfaces to allow MAC address changes and to accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate interfaces and the same interfaces on the different VM instances in the cluster will have the same virtual MAC addresses.

To make the required changes in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect FortiGate VM interfaces.
4. Set **MAC Address Changes**to**Accept**.
5. Set **Forged Transmits** to **Accept**.

Power on your FortiGate VM

You can now proceed to power on your FortiGate VM. There are several ways to do this:

- Select the name of the FortiGate VM you deployed in the inventory list and select **Power on the virtual machine** in the **Getting Started** tab.
- In the inventory list, right-click the name of the FortiGate VM you deployed, and select **Power > Power On**.
- Select the name of the FortiGate VM you deployed in the inventory list. Click the **Power On** button on the toolbar.

Select the Console tab to view the console. To enter text, you must click in the console pane. The mouse is then captured and cannot leave the console screen. As the FortiGate console is text-only, no mouse pointer is visible. To release the mouse, press Ctrl-Alt.

Deployment example – MS Hyper-V

Once you have downloaded the FGT_VMxx_HV-v5-build0xxx-FORTINET.out.hyperv.zip file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

The following topics are included in this section:

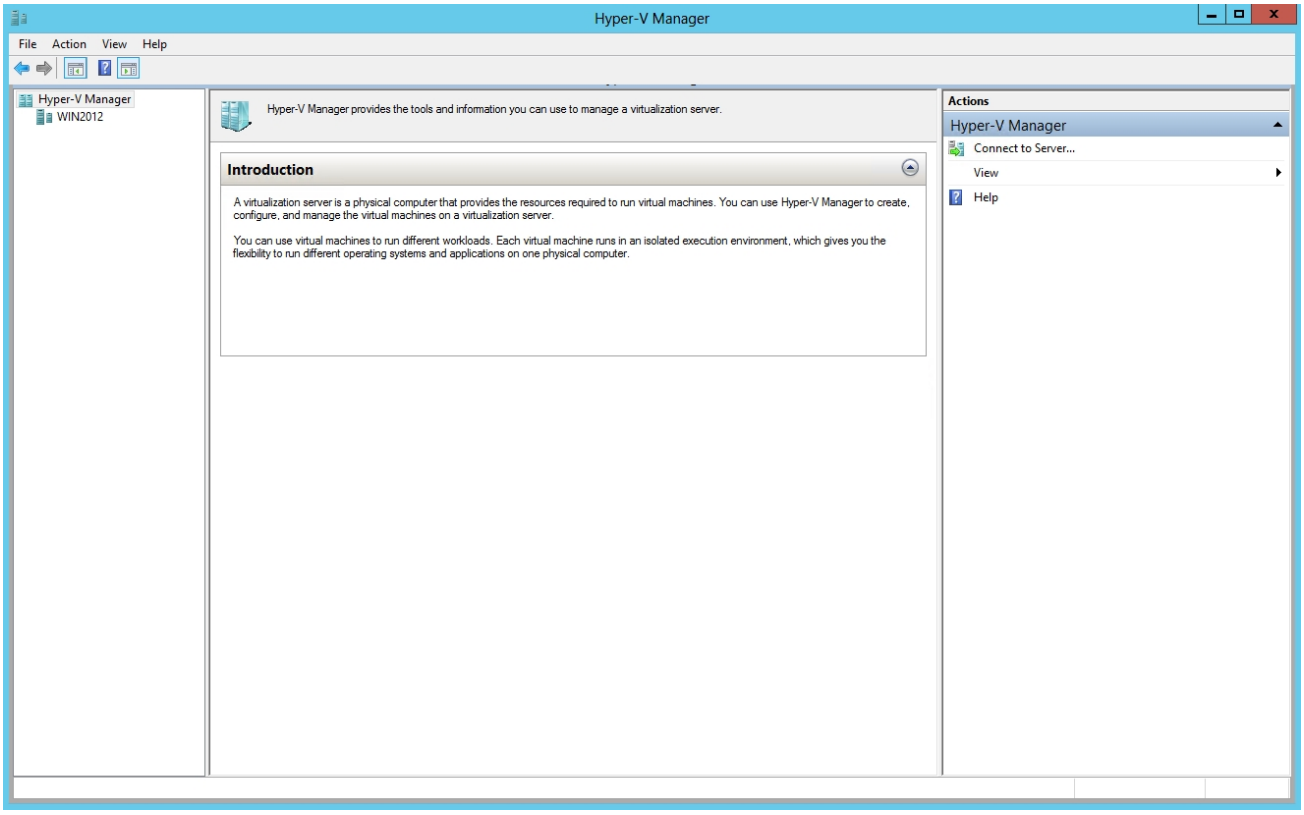
Create the FortiGate VM virtual machine
Configure FortiGate VM hardware settings
High Availability Hyper-V configuration
Start the FortiGate VM

Create the FortiGate VM virtual machine

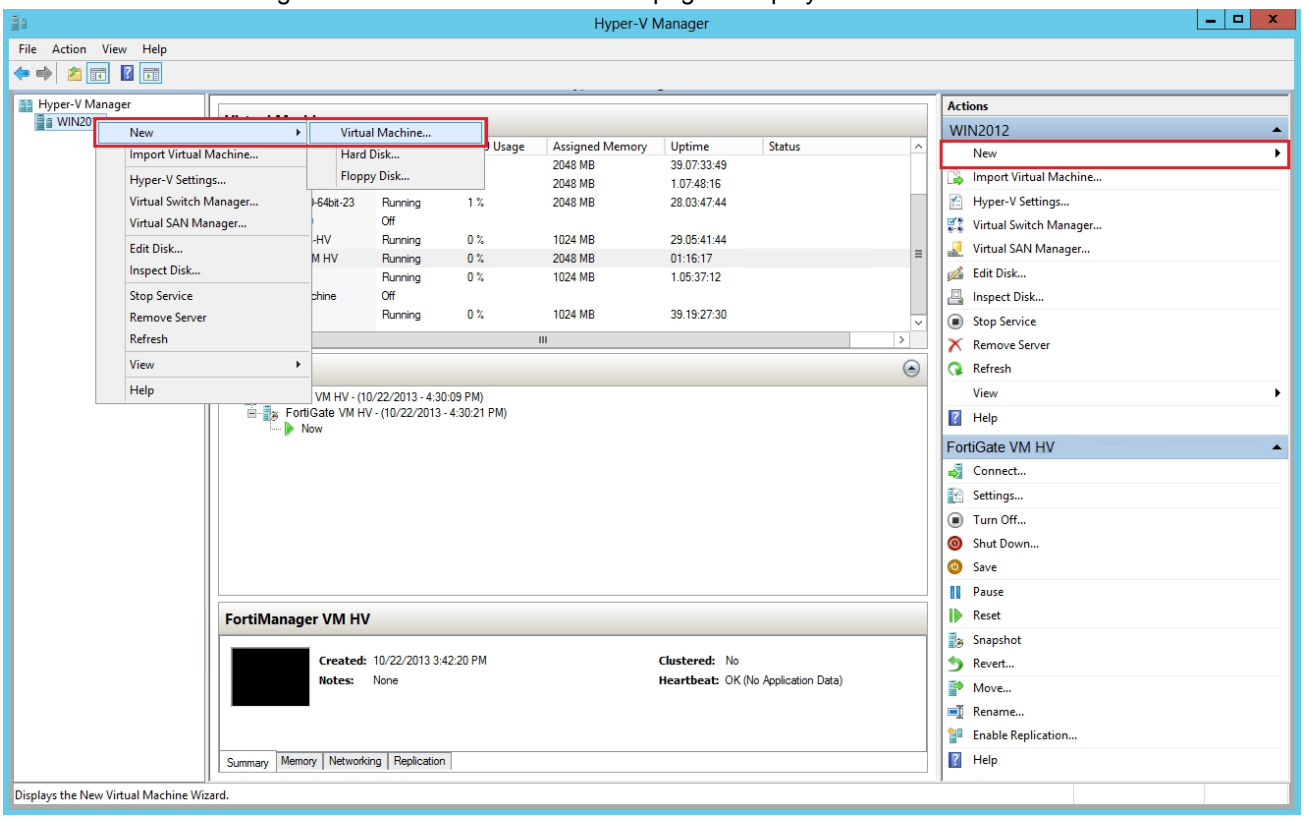
To create the FortiGate VM virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server.

   The **Hyper-V Manager** home page opens.

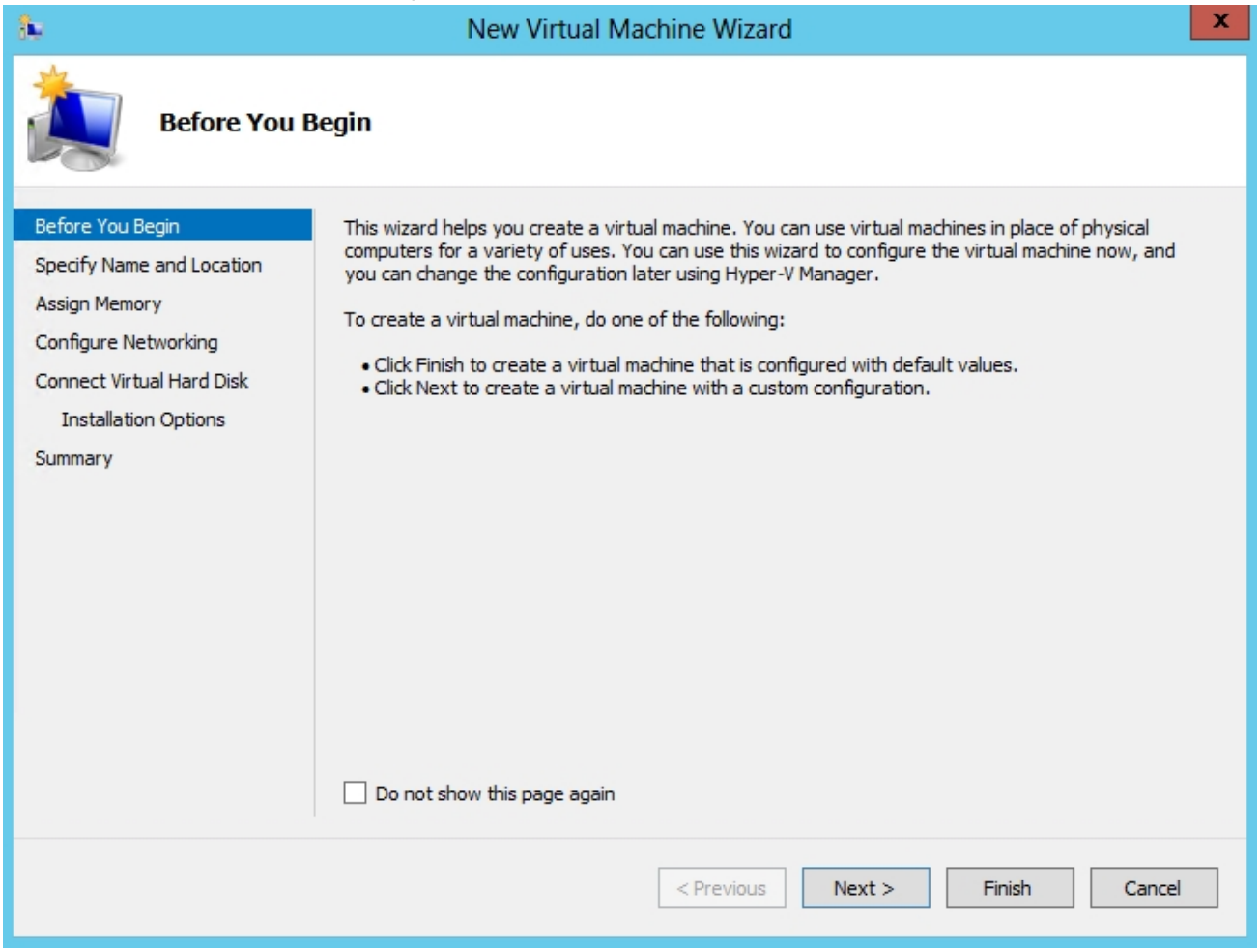


2. Select the server in the right-tree menu. The server details page is displayed.



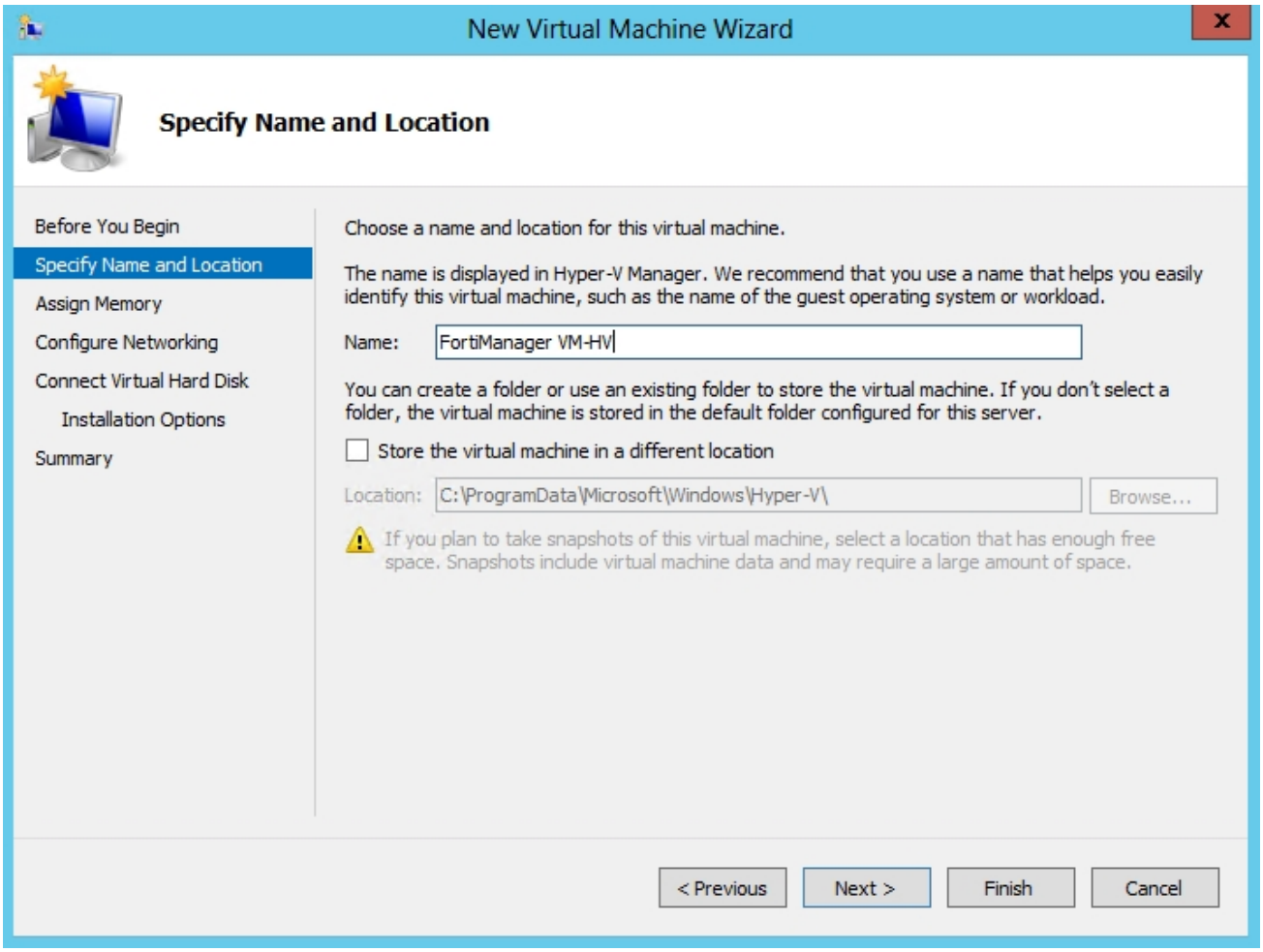
3. Right-click the server and select **New and select Virtual Machine** from the menu. Optionally, in the **Actions** menu, select **New** and select **Virtual Machine** from the menu.

The **New Virtual Machine Wizard** opens.



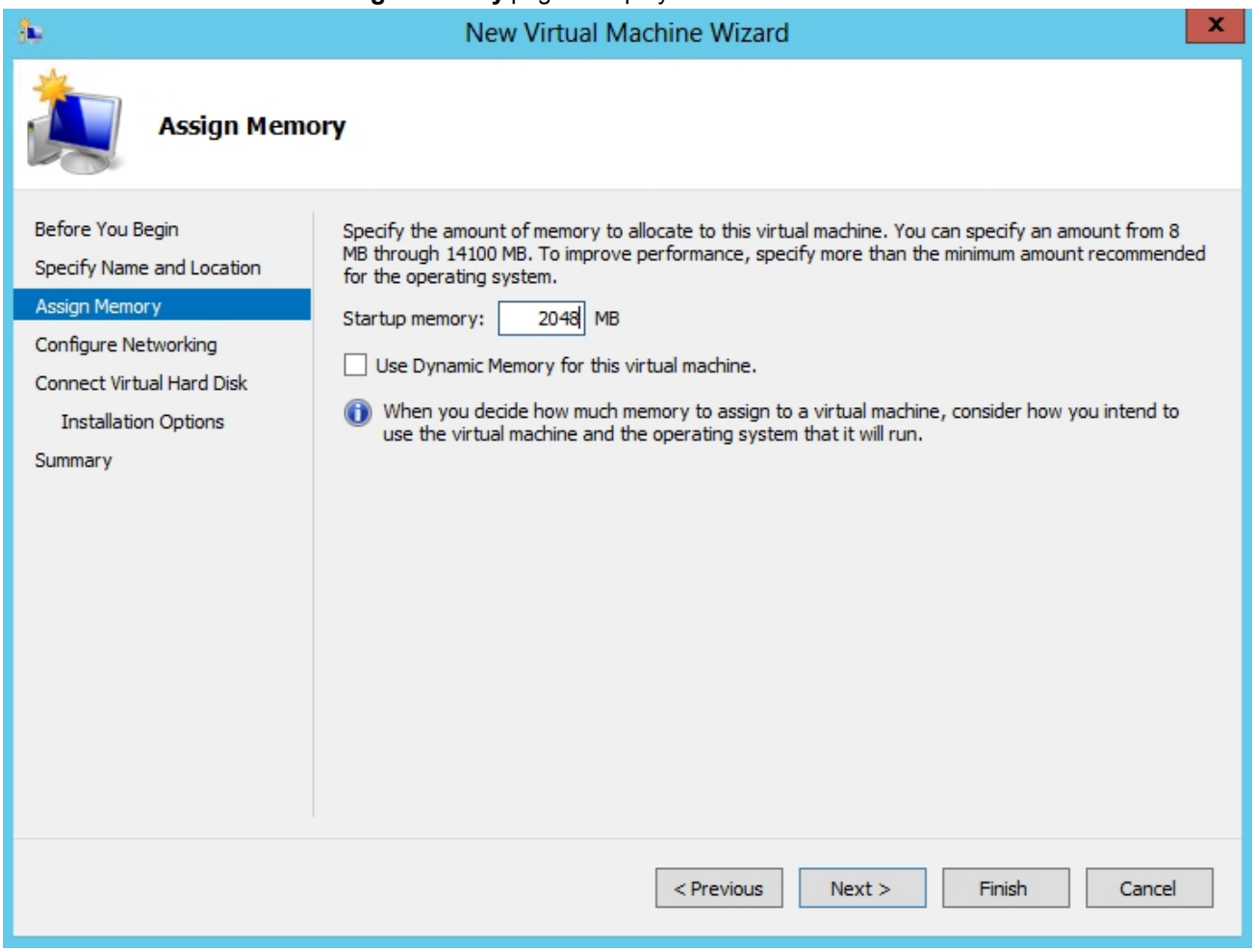
4. Select **Next** to create a virtual machine with a custom configuration.

   The **Specify Name and Location** page is displayed.



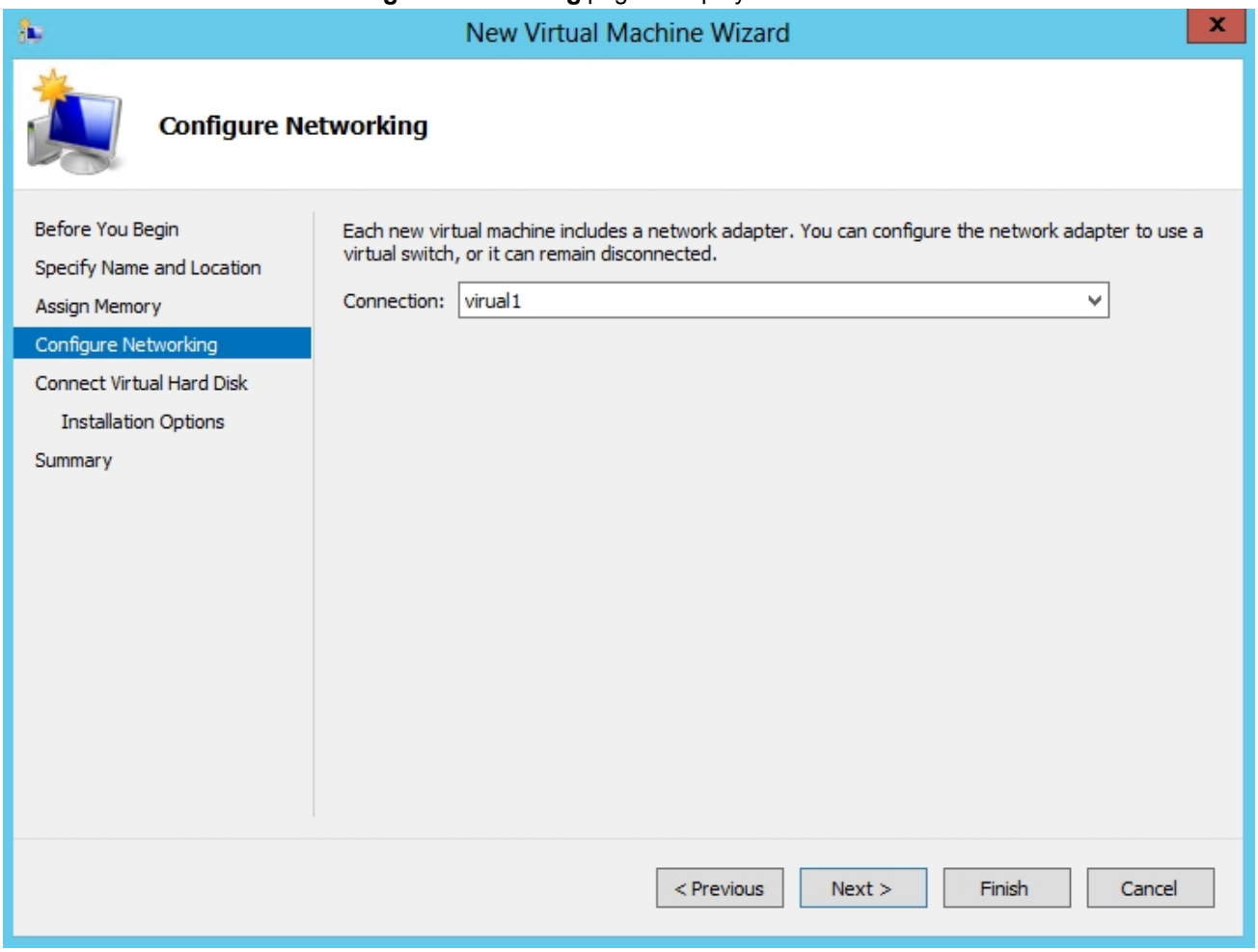
5. Enter a name for this virtual machine. The name is displayed in the Hyper-V Manager.

Select **Next** to continue. The **Assign Memory** page is displayed.



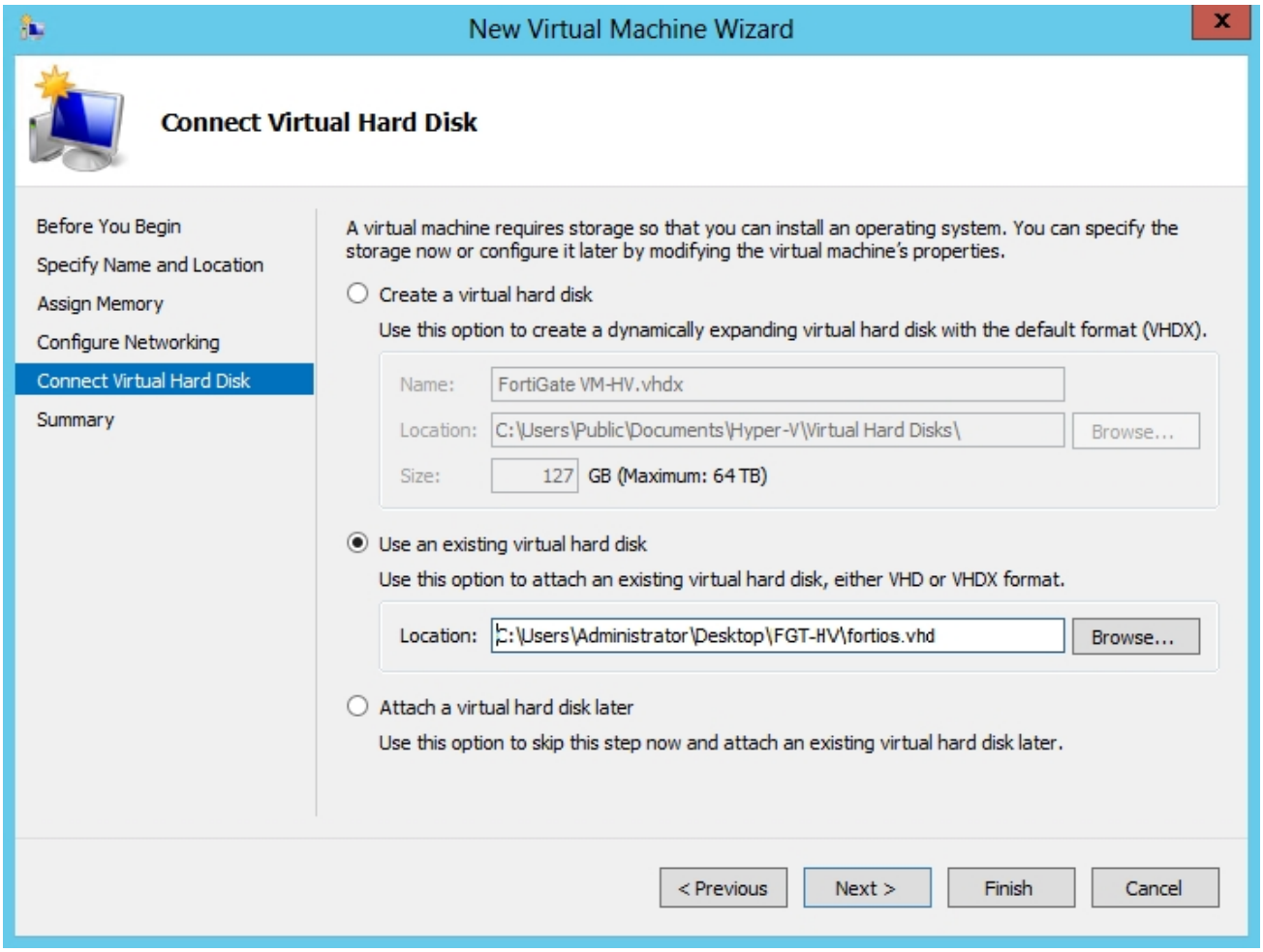
6. Specify the amount of memory to allocate to this virtual machine. The default memory for FortiGate VM is 1GB (1024MB).

Select **Next** to continue. The **Configure Networking** page is displayed.



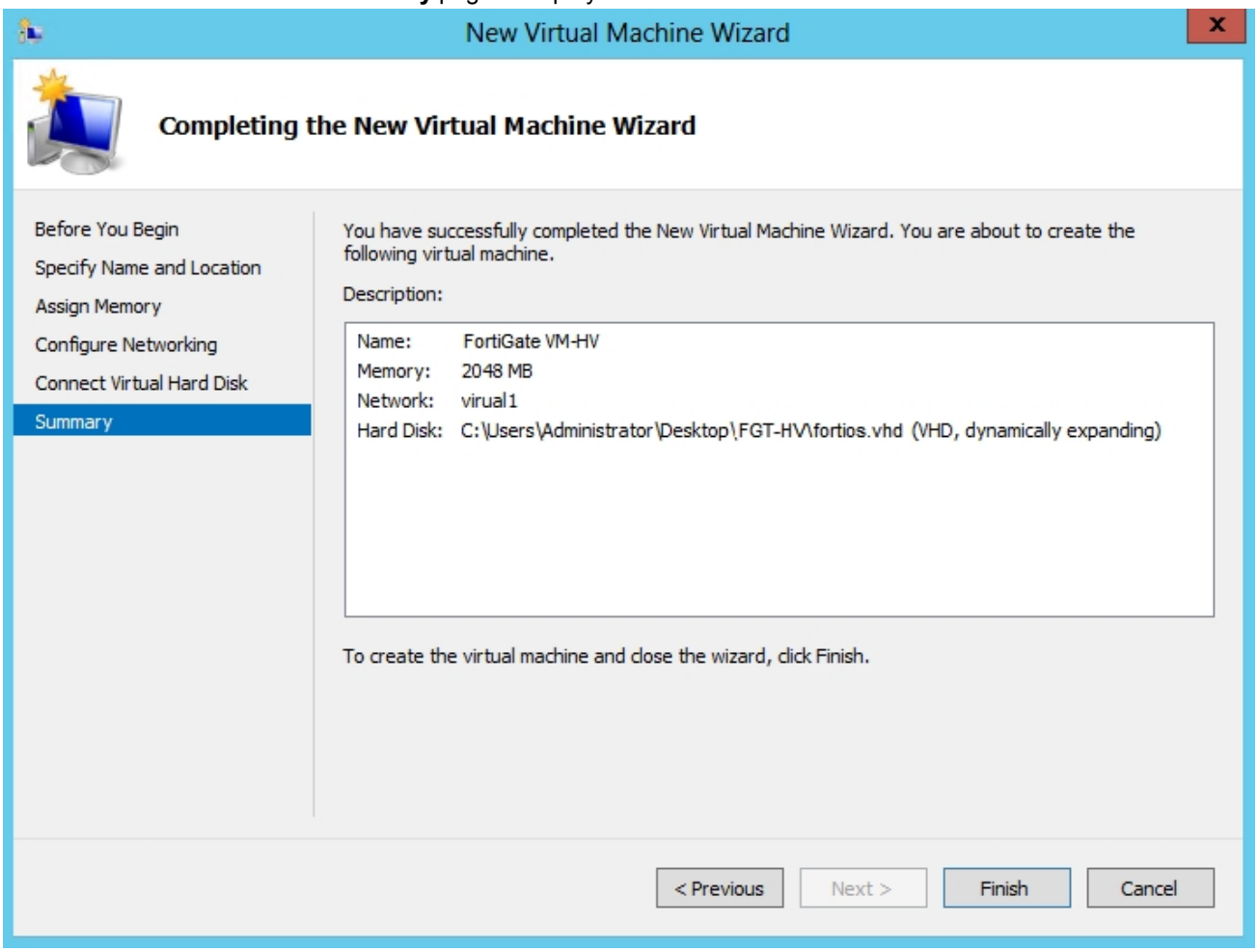
7. Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiGate VM requires four network adapters. You must configure network adapters in the **Settings** page.

   Select **Next** to continue. The **Connect Virtual Hard Disk** page is displayed.



8. Select to use an existing virtual hard disk and browse for the `fortios.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.

Select **Next** to continue. The **Summary** page is displayed.



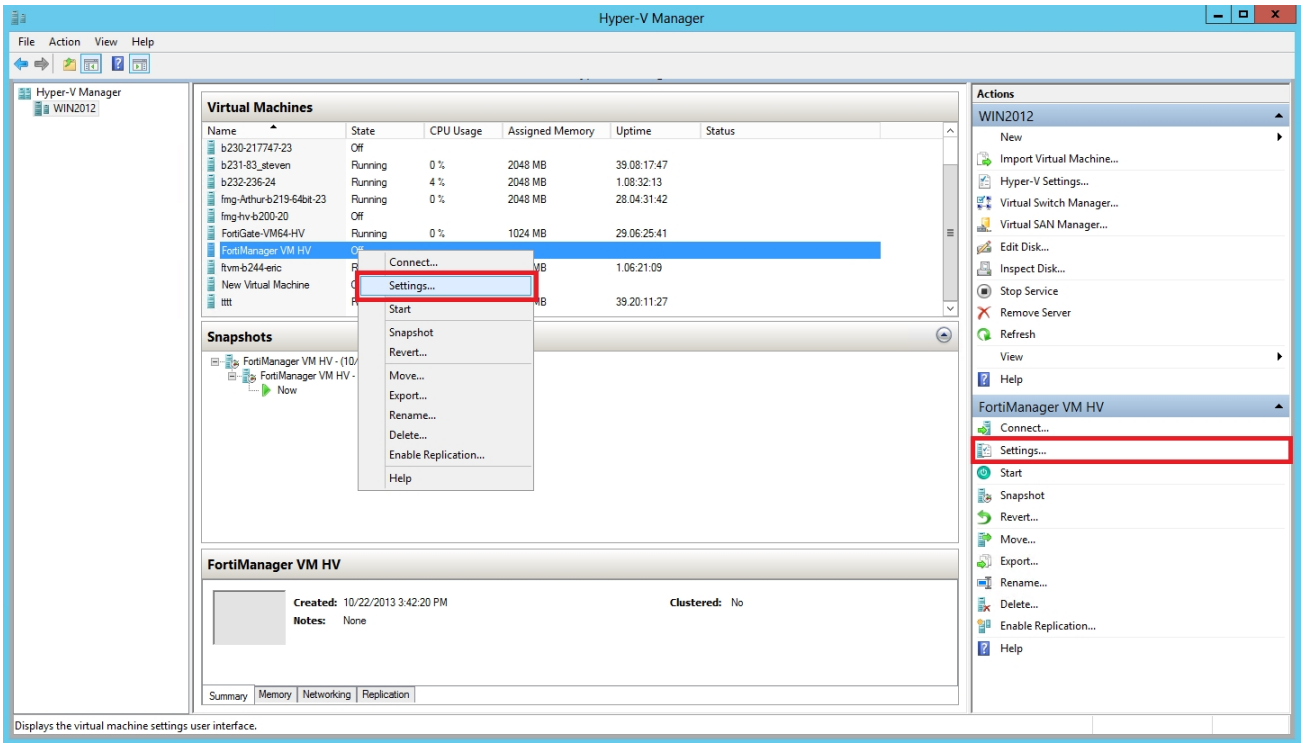
9. To create the virtual machine and close the wizard, select **Finish**.

Configure FortiGate VM hardware settings

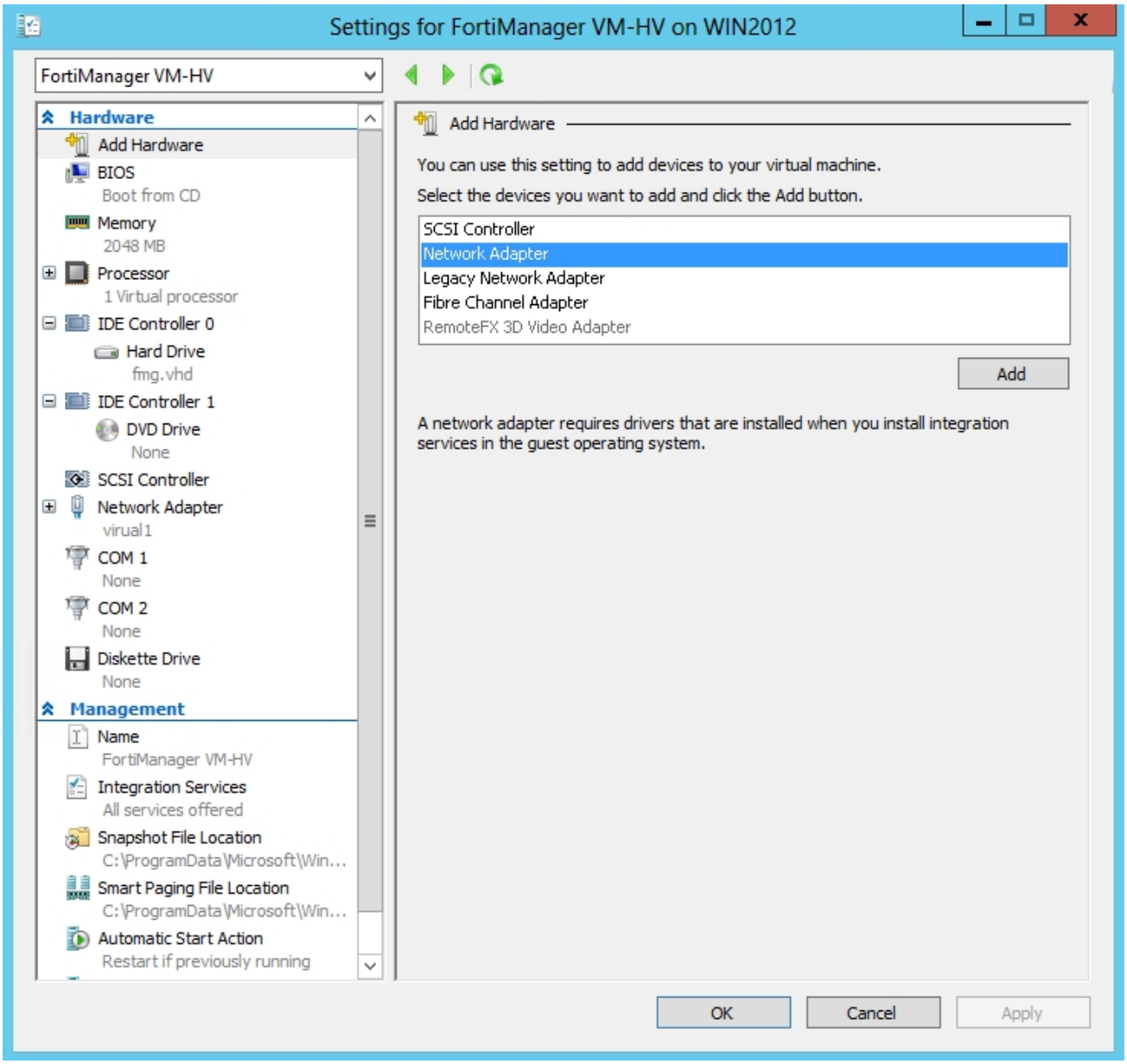
Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.

To configure settings for FortiGate VM on the server:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select **Settings** from the menu. Optionally, you can select the virtual machine and select **Settings** in the **Actions** menu.



The **Settings** page is displayed.



2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select **Apply** to save the settings and then select **OK** to close the settings page.

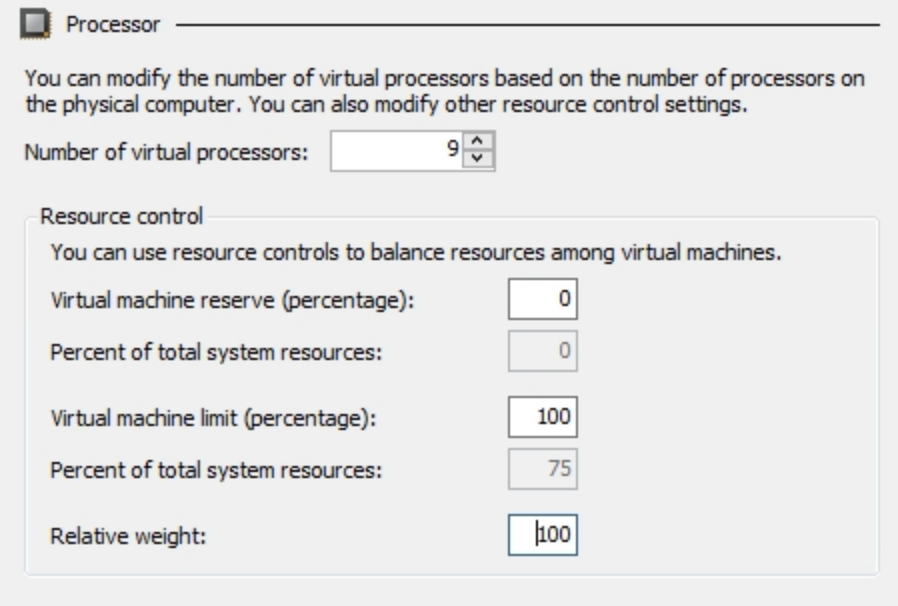
FortiGate VM virtual processors

You must configure FortiGate VM virtual processors in the server settings page. The number of processors is dependent on your server environment.

Configure FortiGate VM virtual processors:

1. In the **Settings** page, select **Processor** from the **Hardware** menu.

   The **Processor** page is displayed.



2. Configure the number of virtual processors for the FortiGate VM virtual machine. Optionally, you can use resource controls to balance resources among virtual machines.
3. Select **Apply** to save the settings.

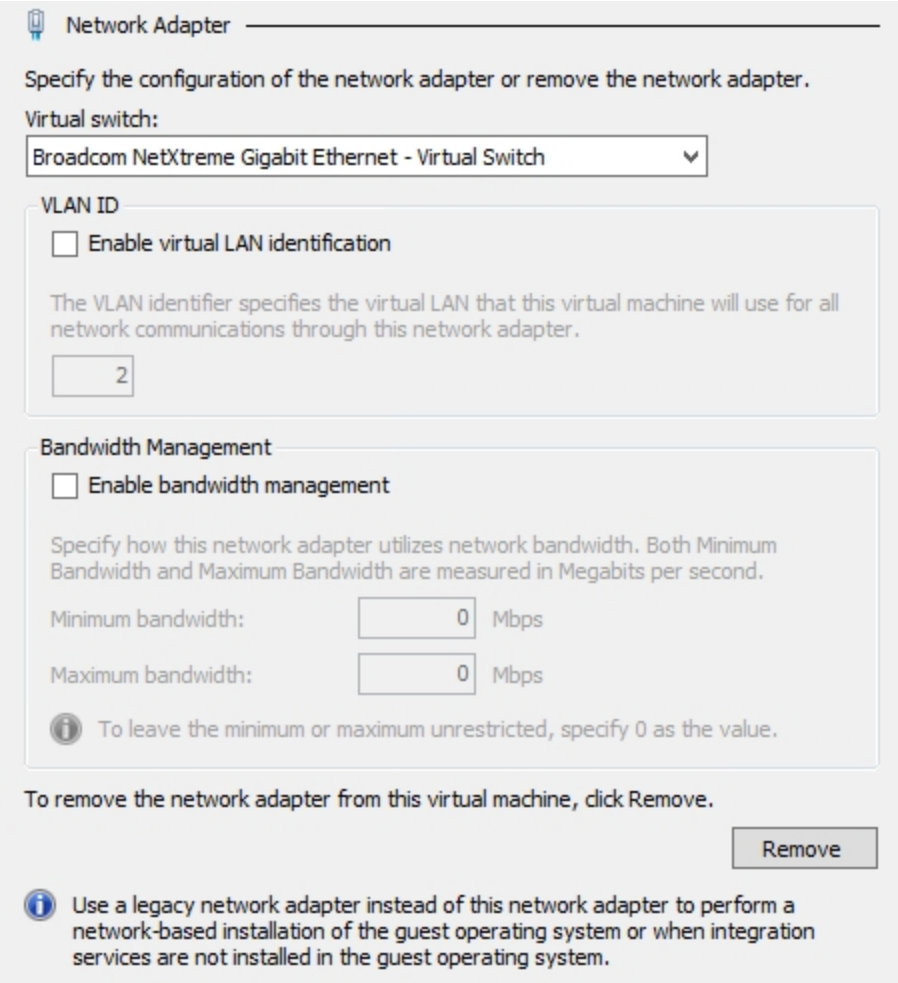
FortiGate VM network adapters

You must configure FortiGate VM network adapters in the server settings page. FortiGate VM supports four network adapters.

Configure FortiGate VM network adapters:

1. In the **Settings** page, select **Add Hardware** from the **Hardware** menu, select **Network Adapter** in the device list, and select the **Add** button.

The **Network Adapter** page is displayed.



1. You must manually configure four network adapters for FortiGate VM in the settings page. For each network adapter, select the virtual switch from the drop-down list.
2. Select **Apply** to save the settings.

FortiGate VM virtual hard disk

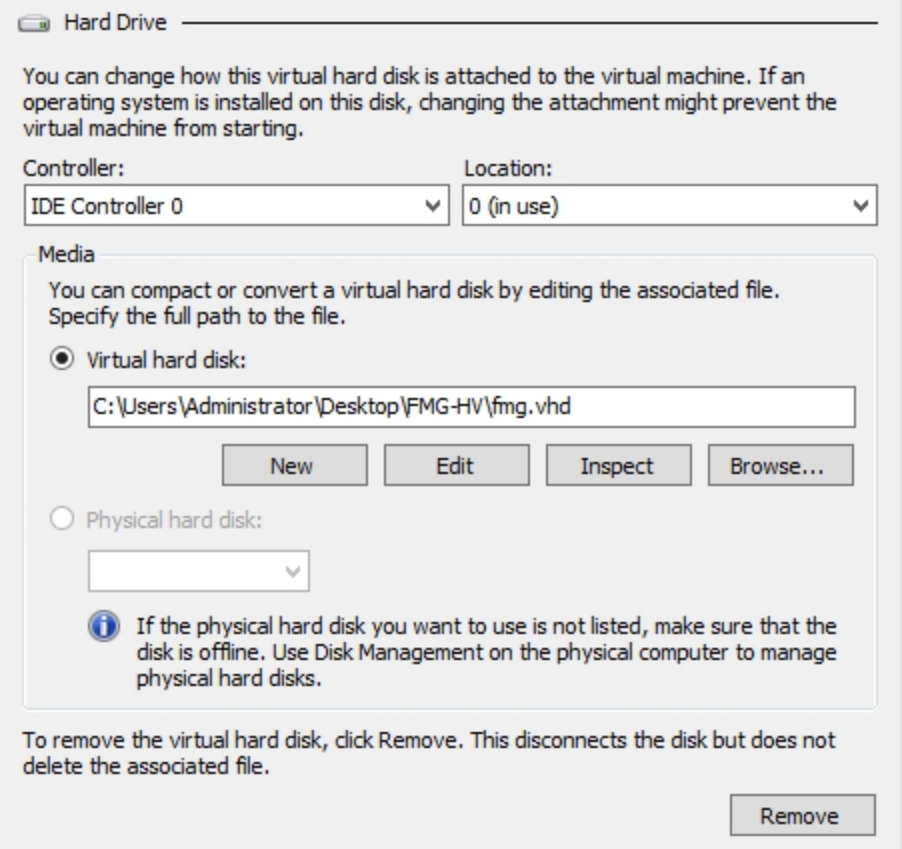
You must configure the FortiGate VM virtual hard disk in the server settings page.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

Configure a FortiGate VM virtual hard drive:

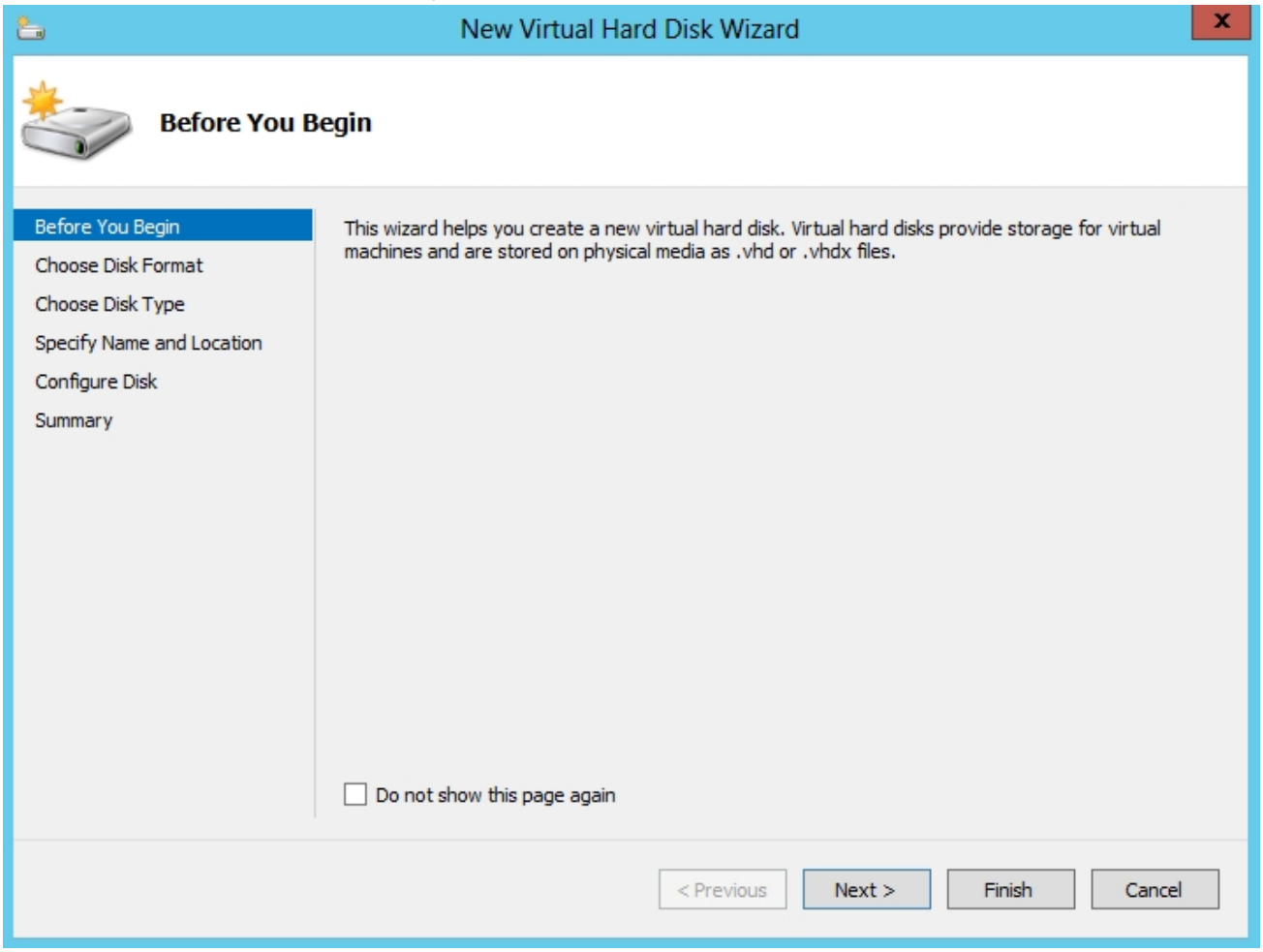
1. In the **Settings** page, select **IDE Controller 0 > Hard Drive** from the **Hardware** menu.

   The **Hard Drive** page is displayed.



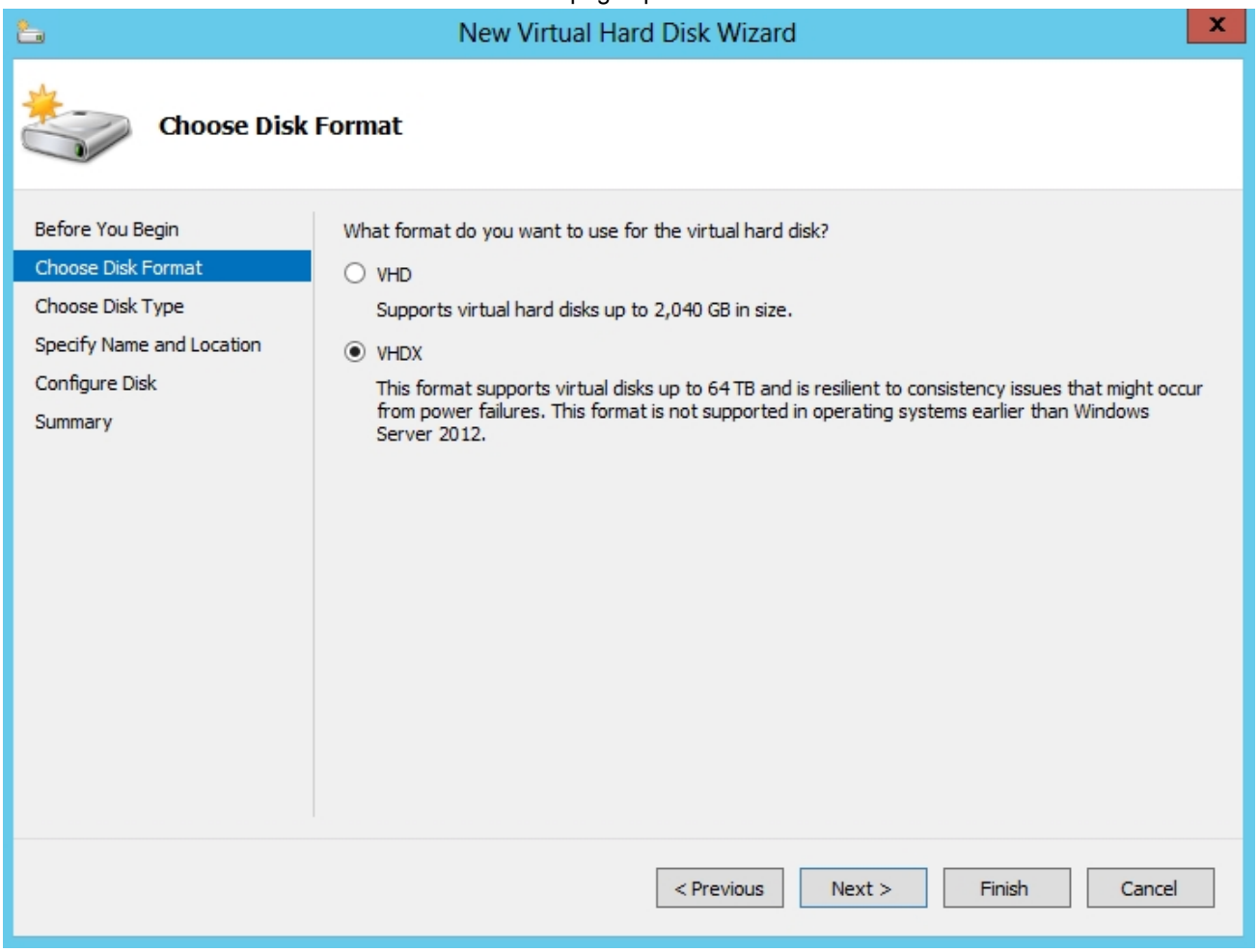
2. Select **New** to create a new virtual hard disk.

The **New Virtual Hard Disk Wizard** opens.



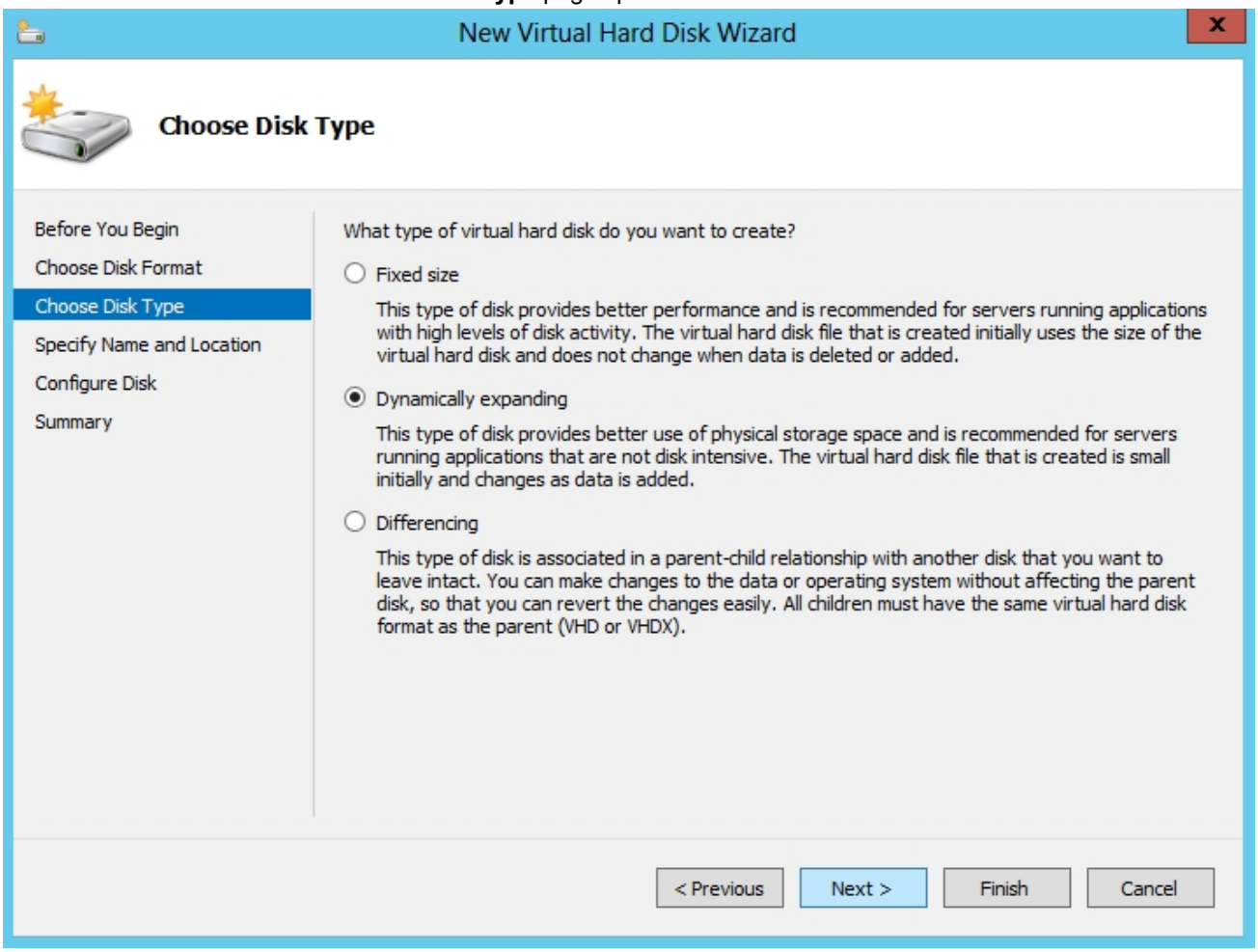
3. This wizard helps you to create a new virtual hard disk.

Select **Next** to continue. The **Choose Disk Format** page opens.



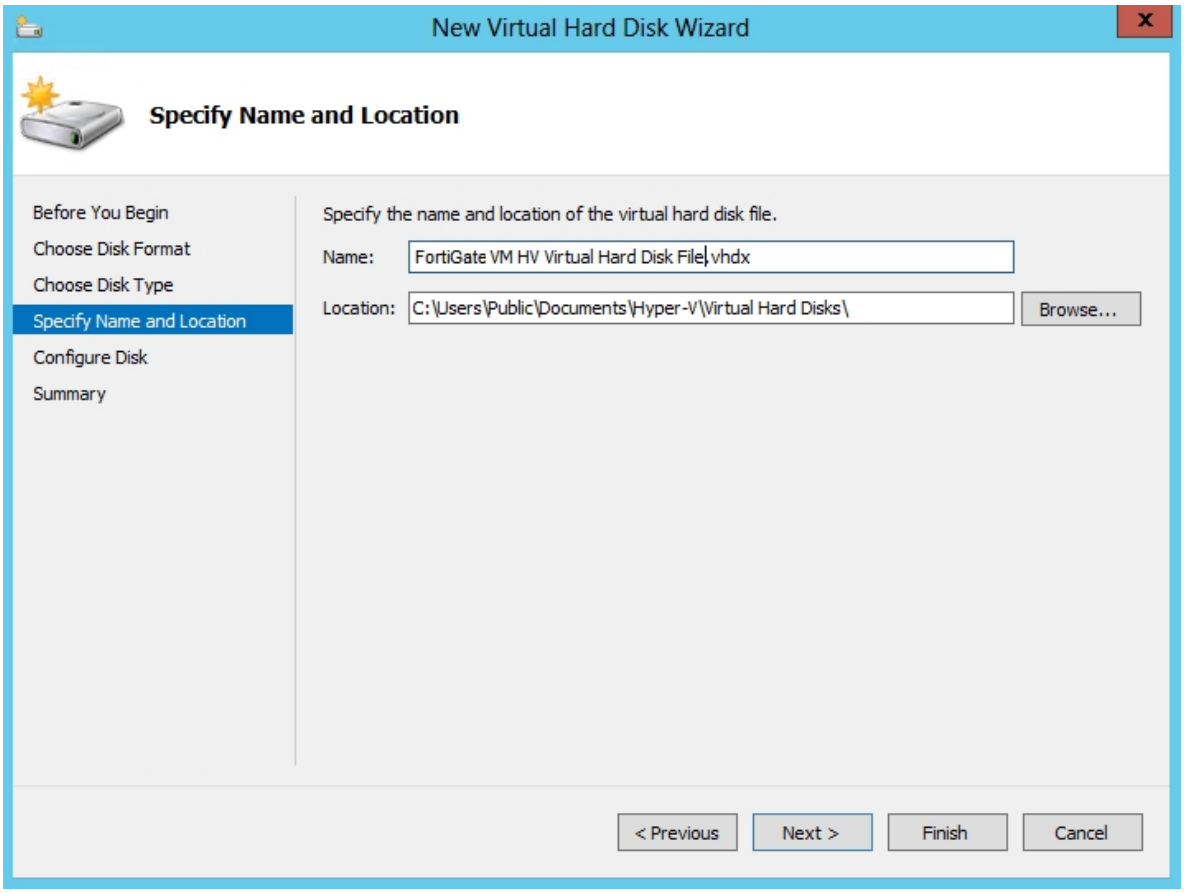
4. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. Note that FortiGate-VM does not support hard disks larger than 2TB.

Select **Next** to continue. The **Choose Disk Type** page opens.



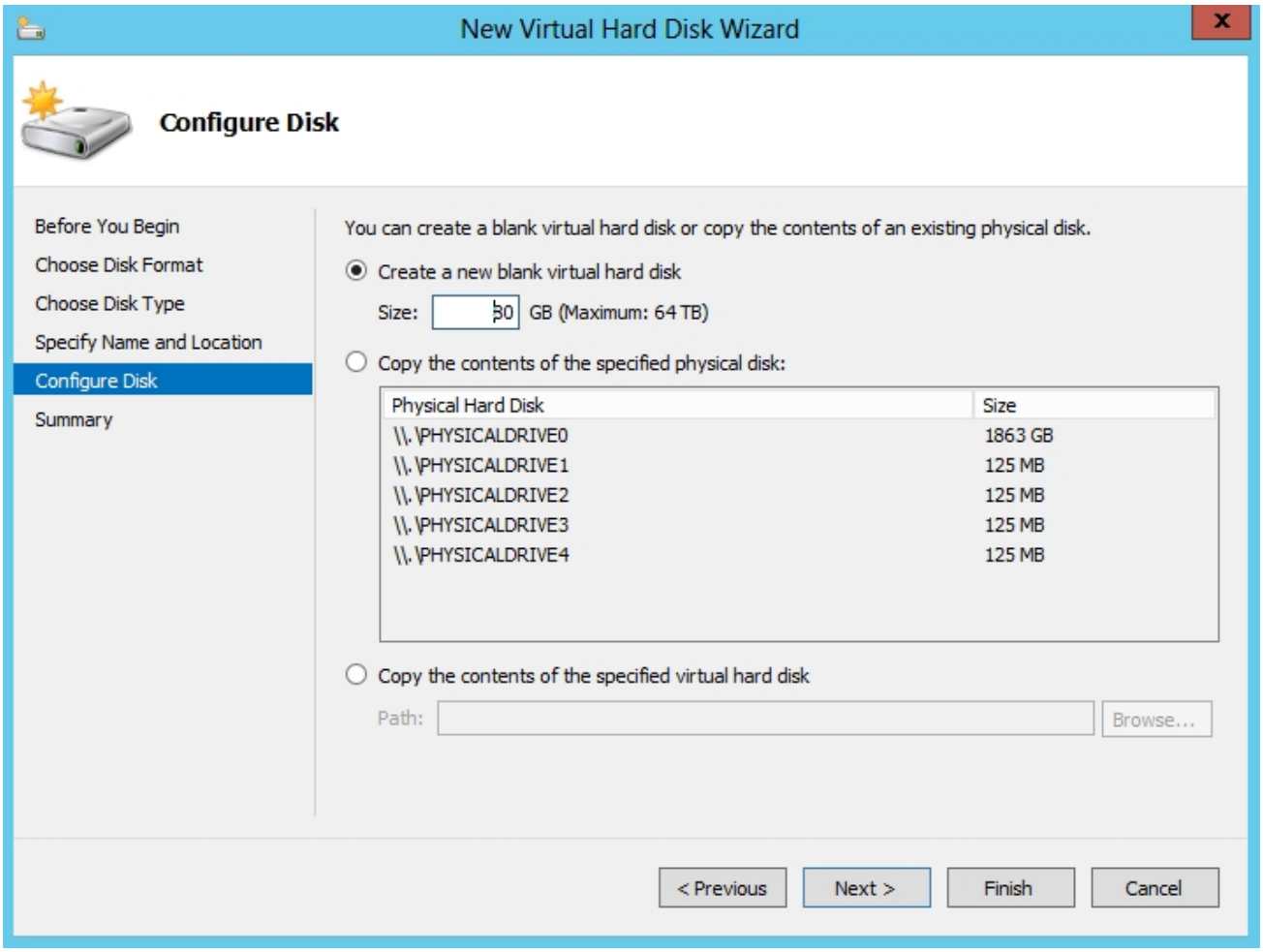
5. Select the type of virtual disk you want to use. Select one of the following disk types:
   - Fixed size: This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
   - Dynamic expanding: This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
   - Differencing: This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

   Select **Next** to continue. The **Specify Name and Location** page opens.



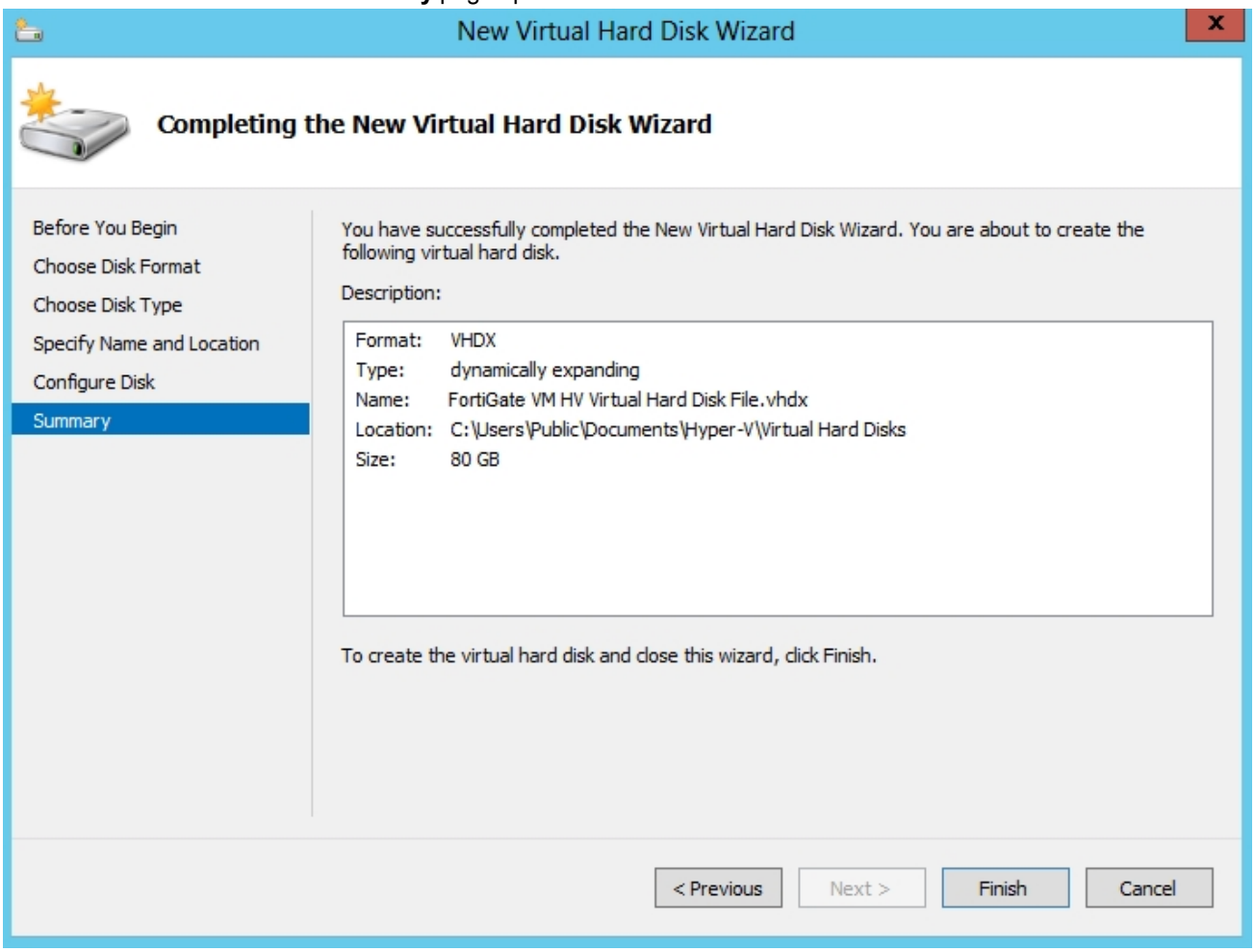
6. Specify the name and location of the virtual hard disk file. Use the **Browse** button to select a specific file folder on your server.

   Select **Next** to continue. The **Configure Disk** page opens.



7. Select to **Create a new blank virtual hard disk** and enter the size of the disk in GB. The maximum size is dependent on your server environment.

Select **Next** to continue. The **Summary** page opens.



8. The summary page provides details of the virtual hard disk. Select **Finish** to create the virtual hard disk.
9. Select **Apply** to save the settings and select **OK** to exit the settings page.

High Availability Hyper-V configuration

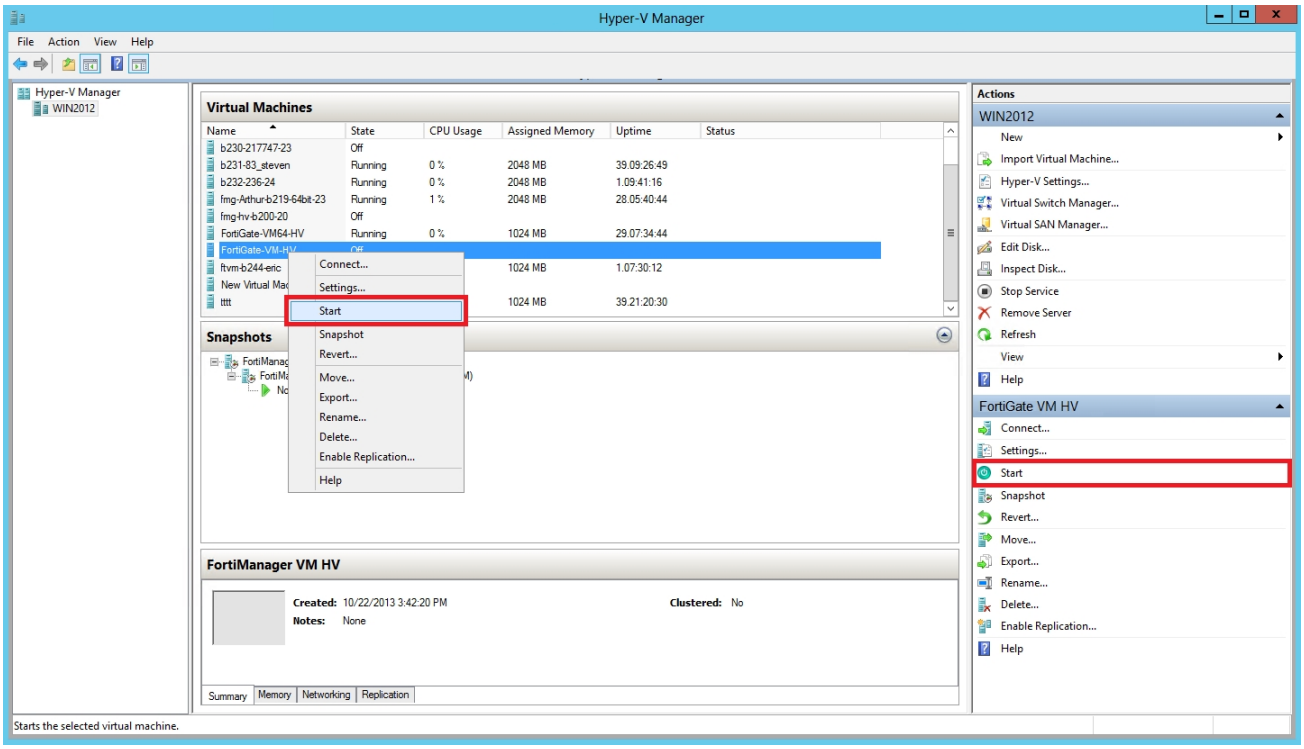
Promiscuous mode and support for MAC address spoofing is required for FortiGate-VM for Hyper-V to support FortiGate Clustering Protocol (FGCP) high availability (HA). By default the FortiGate-VM for Hyper-V has promiscuous mode enabled in the XML configuration file in the FortiGate-VM Hyper-V image. If you have problems with HA mode, confirm that this is still enabled.

In addition, because the FGCP applies virtual MAC addresses to FortiGate data interfaces and because these virtual MAC addresses mean that matching interfaces of different FortiGate-VM instances will have the same virtual MAC addresses you have to configure Hyper-V to allow MAC spoofing. But you should only enable MAC spoofing for FortiGate-VM data interfaces. You should not enable MAC spoofing for FortiGate HA heartbeat interfaces.

With promiscuous mode enabled and the correct MAC spoofing settings you should be able to configure HA between two or more FortiGate-VM for Hyper-V instances.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines, right-click, and select **Start** in the menu. Optionally, you can select the name of the FortiGate VM in the list of virtual machines and select **Start** in the **Actions** menu.



Deployment example – KVM

Once you have downloaded the FORTINET.out.kvm.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your KVM environment.

The following topics are included in this section:

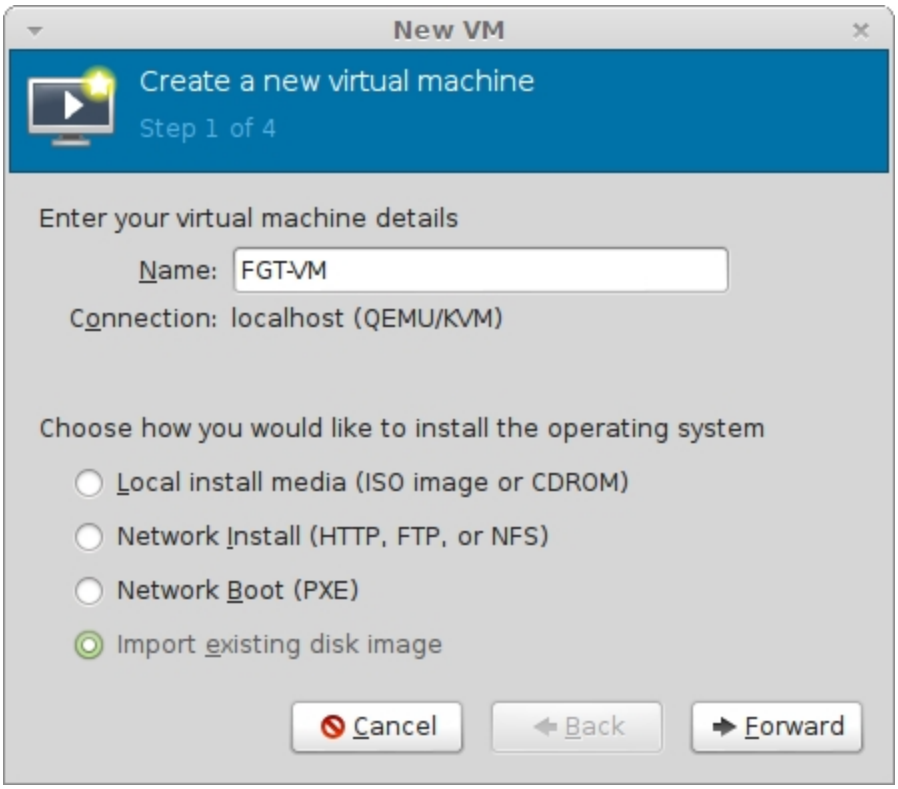
Create the FortiGate VM virtual machine
Configure FortiGate VM hardware settings
Start the FortiGate VM

Create the FortiGate VM virtual machine

To create the FortiGate VM virtual machine:

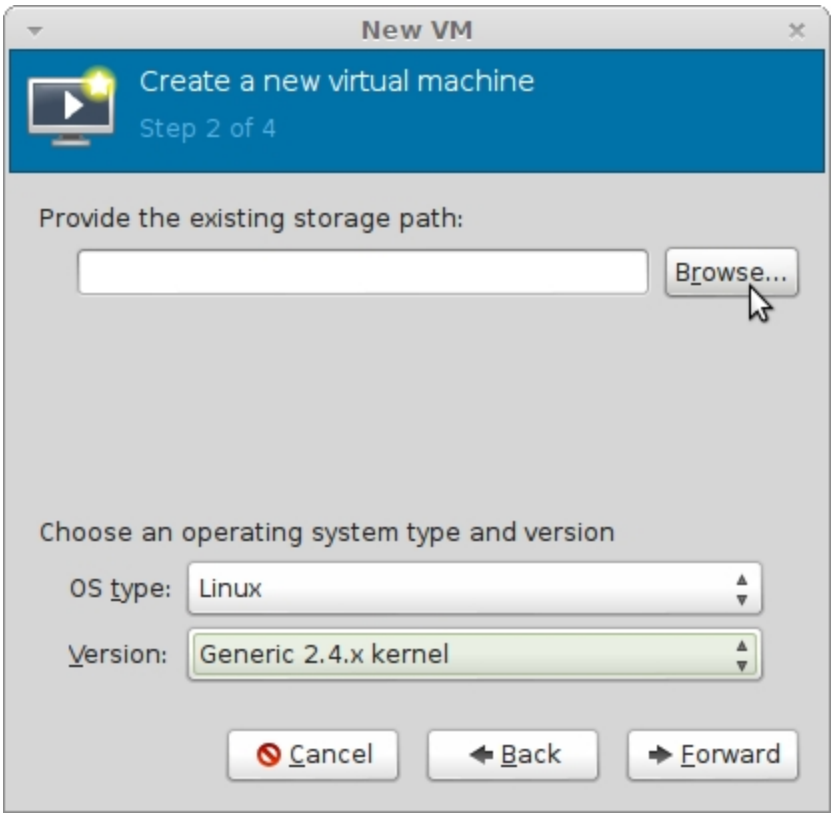
1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.

   The **Virtual Machine Manager** home page opens.
2. In the toolbar, select **Create a new virtual machine**.



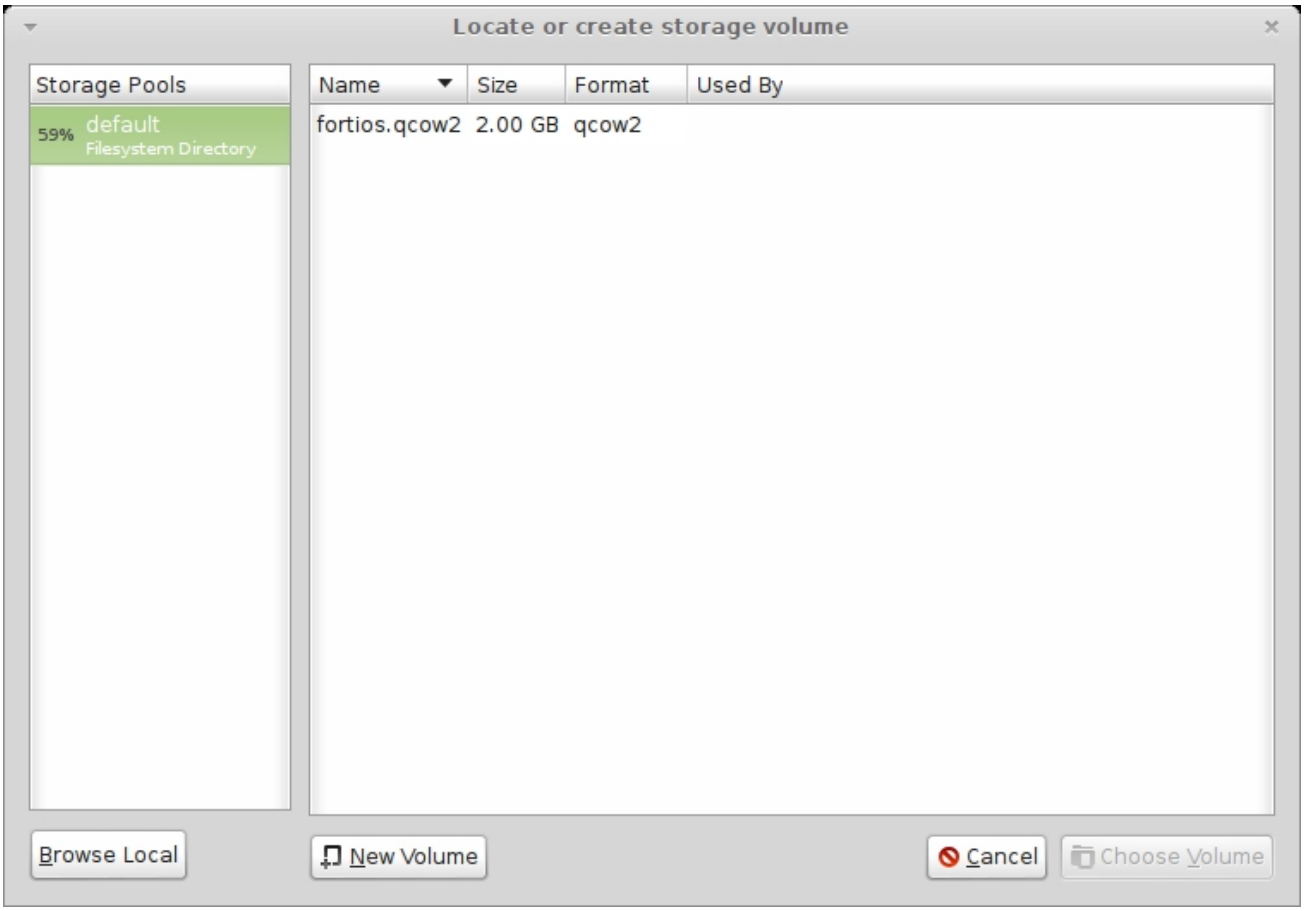
3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.
8. In **Version**, select **Generic 2.4.x.kernel**.

9. Select **Browse**.



10. If you copied the fortios.qcow2 file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select Browse Local and find it.
11. Choose **Choose Volume**.
12. Select **Forward**.
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. See FortiGate VM Overview on page 2658.
14. Select **Forward**.
15. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select a network adapter on the host computer. Optionally, set a specific MAC address for the virtual network interface. Set **Virt Type** to **virtio** and **Architecture** to **qcow2**.
16. Select **Finish**.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must add the log disk and configure the virtual hardware of your FortiGate VM.

To configure settings for FortiGate VM on the server:

1. In the Virtual Machine Manager, locate the name of the virtual machine and then select Open from the toolbar.
2. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.

3. Select **Create a disk image on the computer's harddrive** and set the size to 30GB.

   If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

4. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw

   Even though raw is the storage format listed, the qcow2 format is also supported.

5. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

   A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.
6. Select **Finish**.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines. In the toolbar, select **Console** and then select **Start**.

Deployment example – OpenXen

Once you have downloaded the FORTINET.out.OpenXen.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your OpenXen environment.

The following topics are included in this section:

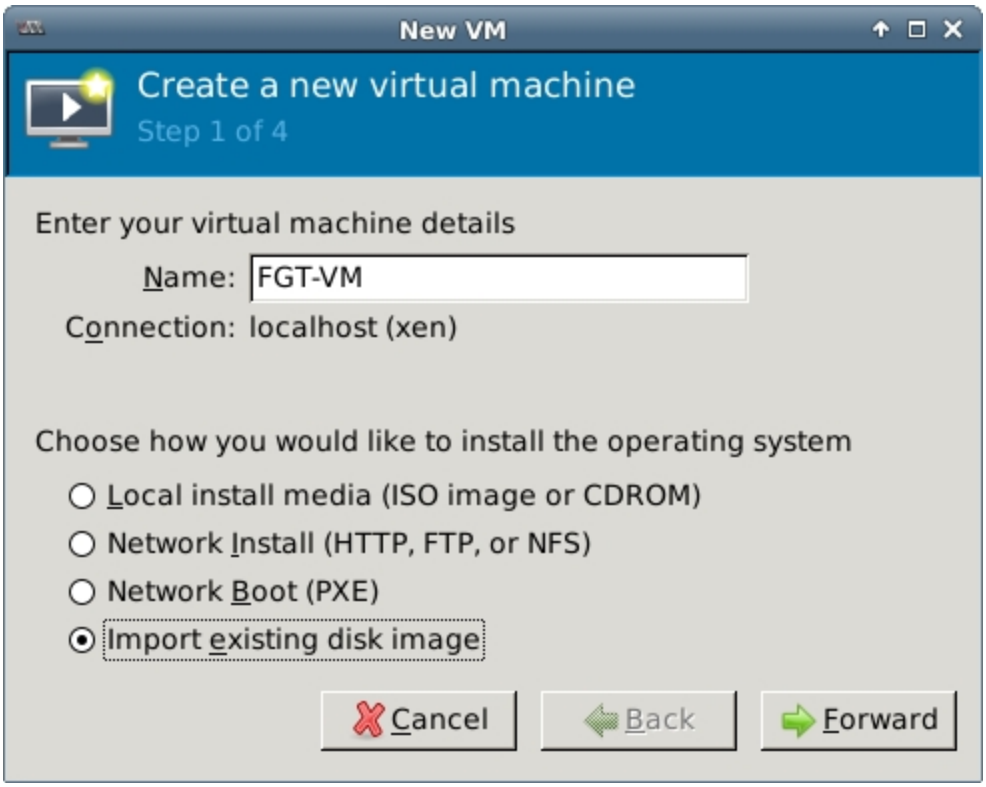
Create the FortiGate VM virtual machine (VMM)

Create the FortiGate VM virtual machine (VMM)

To create the FortiGate VM virtual machine:

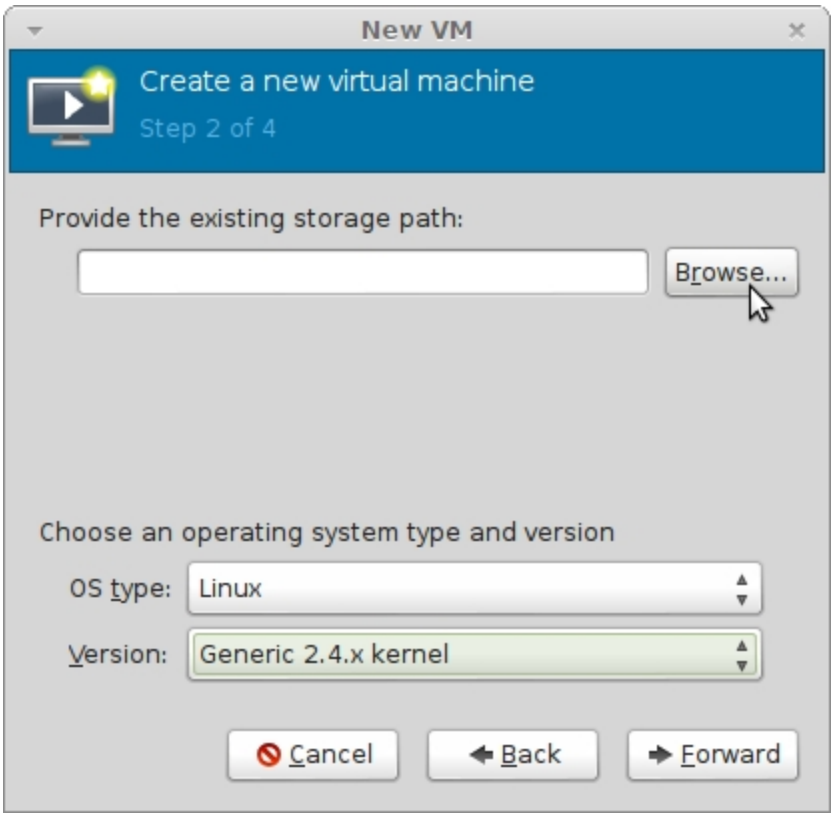
1. Launch Virtual Machine Manager (virt-manager) on your OpenXen host server.

   The **Virtual Machine Manager** home page opens.
2. In the toolbar, select **Create a new virtual machine**.



3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

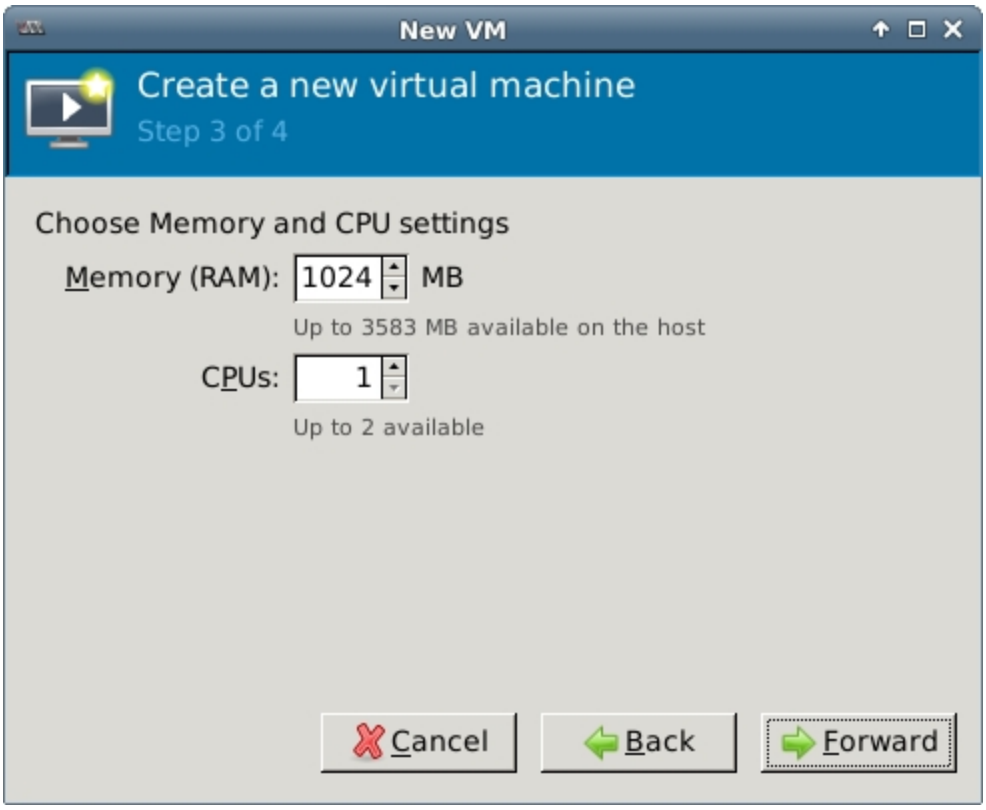
6. Select **Forward**.



7. In **OS Type** select **Linux**.
8. In **Version**, select **Generic 2.4.x.kernel**.
9. Select **Browse**.

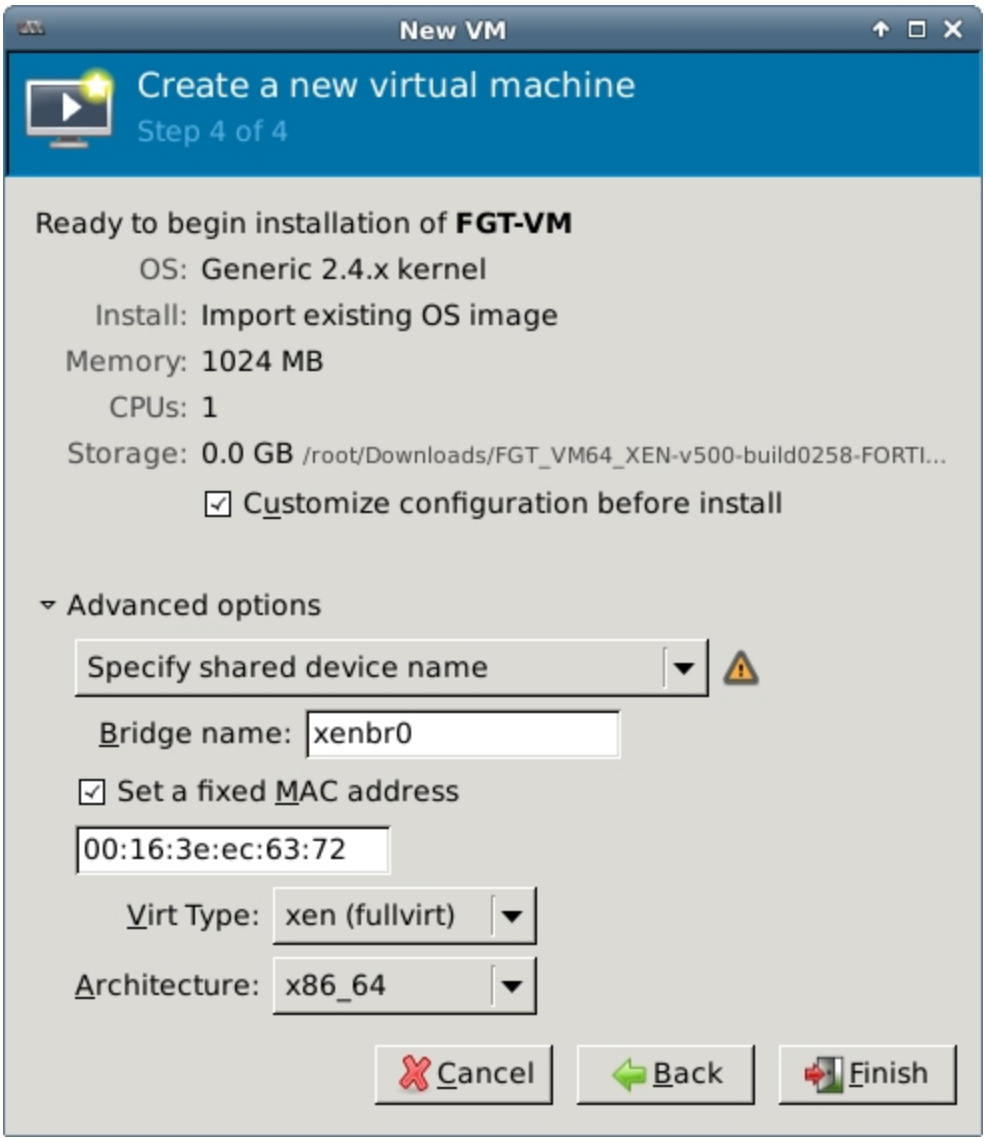
   The **Locate or create storage volume** window opens.
10. Select **Browse Local,** find the fortios.qcow2 disk image file.
11. Select fortios.qcow2 and select **Choose Volume**.

12. Select **Forward**.



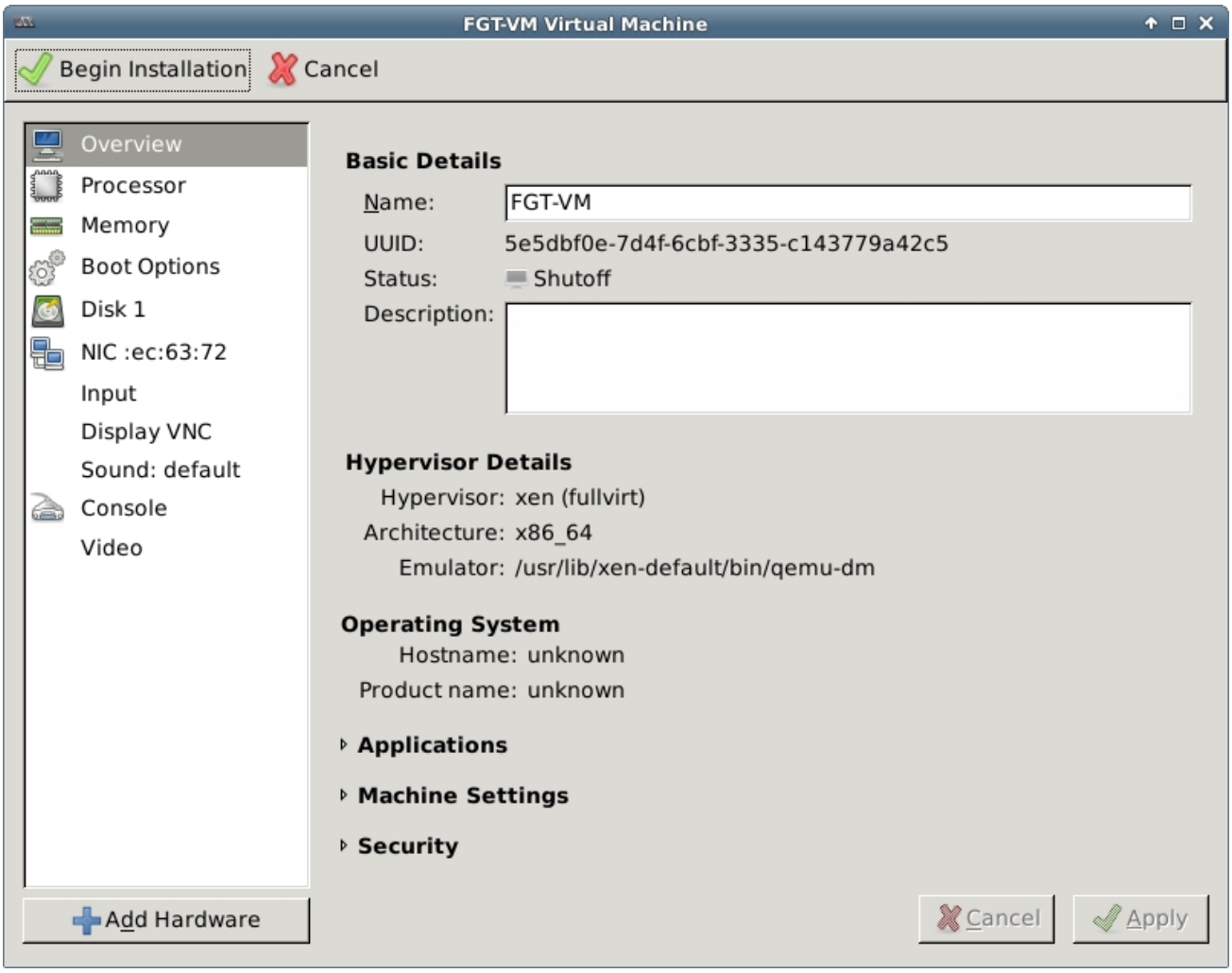
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits.

14. Select **Forward**.



15. Select **Customize configuration before install**. This enables you to make some hardware configuration changes before VM creation is started.
16. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select **Specify shared device name** and enter the name of the bridge interface on the OpenXen host. Optionally, set a specific MAC address for the virtual network interface. **Virt Type** and **Architecture** are set by default and should be correct.
17. Select **Finish**.

    The virtual machine hardware configuration window opens.



You can use this window to add hardware such as network interfaces and disk drives.

18. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.
19. Select **Create a disk image on the computer's harddrive** and set the size to 30GB.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

20. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw

21. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

A new virtual machine includes one network adapter by default. You can add more through the Add Hardware

window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

22. Select **Finish**.
23. Select **Begin Installation**. After the installation completes successfully, the VM starts and the console window opens.

Deployment example – Citrix XenServer

Once you have downloaded the FORTINET.out.CitrixXen.zip file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

Create the FortiGate VM virtual machine (XenCenter)
Configure virtual hardware

Create the FortiGate VM virtual machine (XenCenter)

To create the FortiGate VM virtual machine from the OVF file

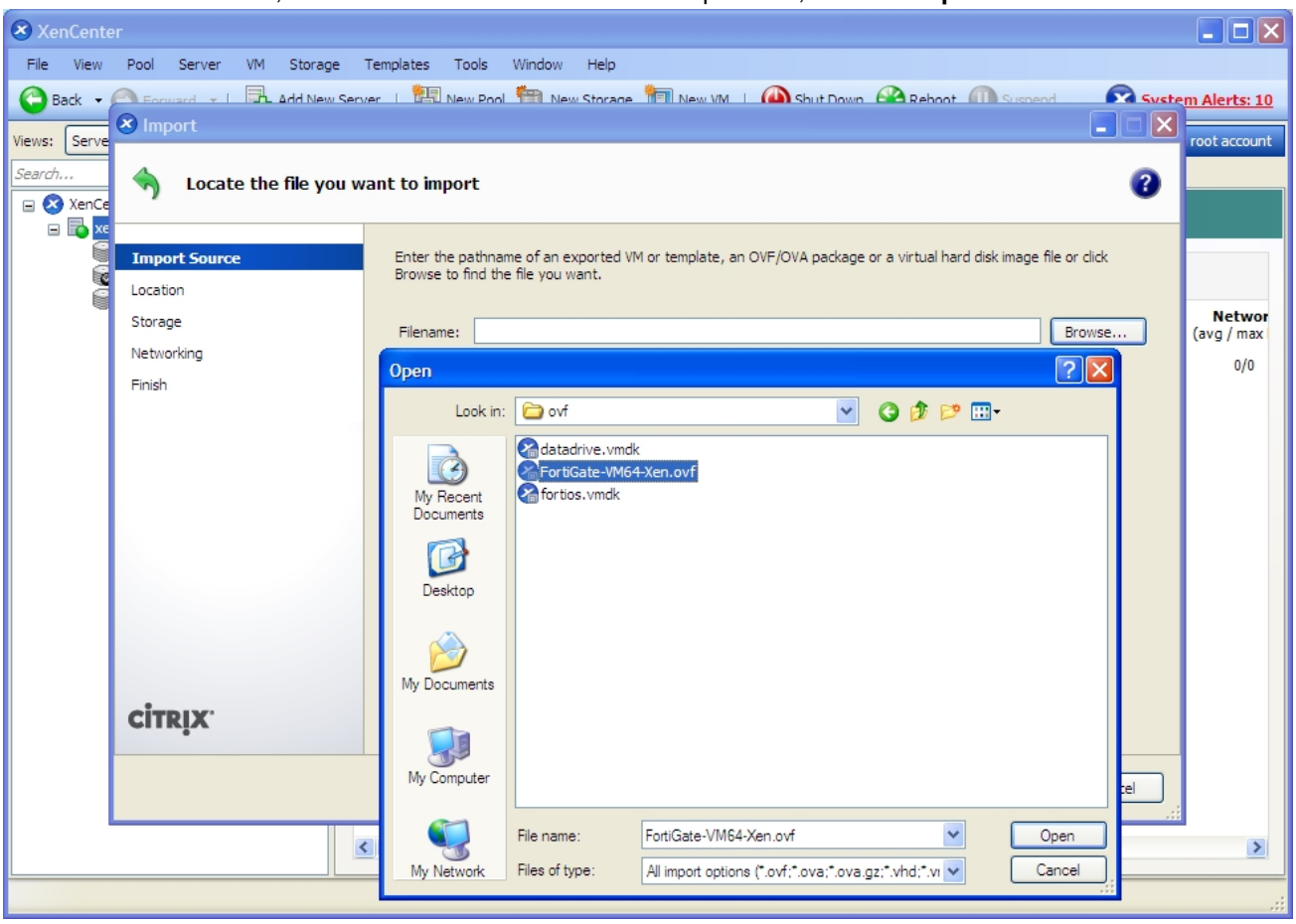
1. Launch XenCenter on your management computer.

   The management computer can be any computer that can run Citrix XenCenter, a Windows application.
2. If you have not already done so, select **ADD a server**. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.

   Your Citrix XenServer is added to the list in the left pane.

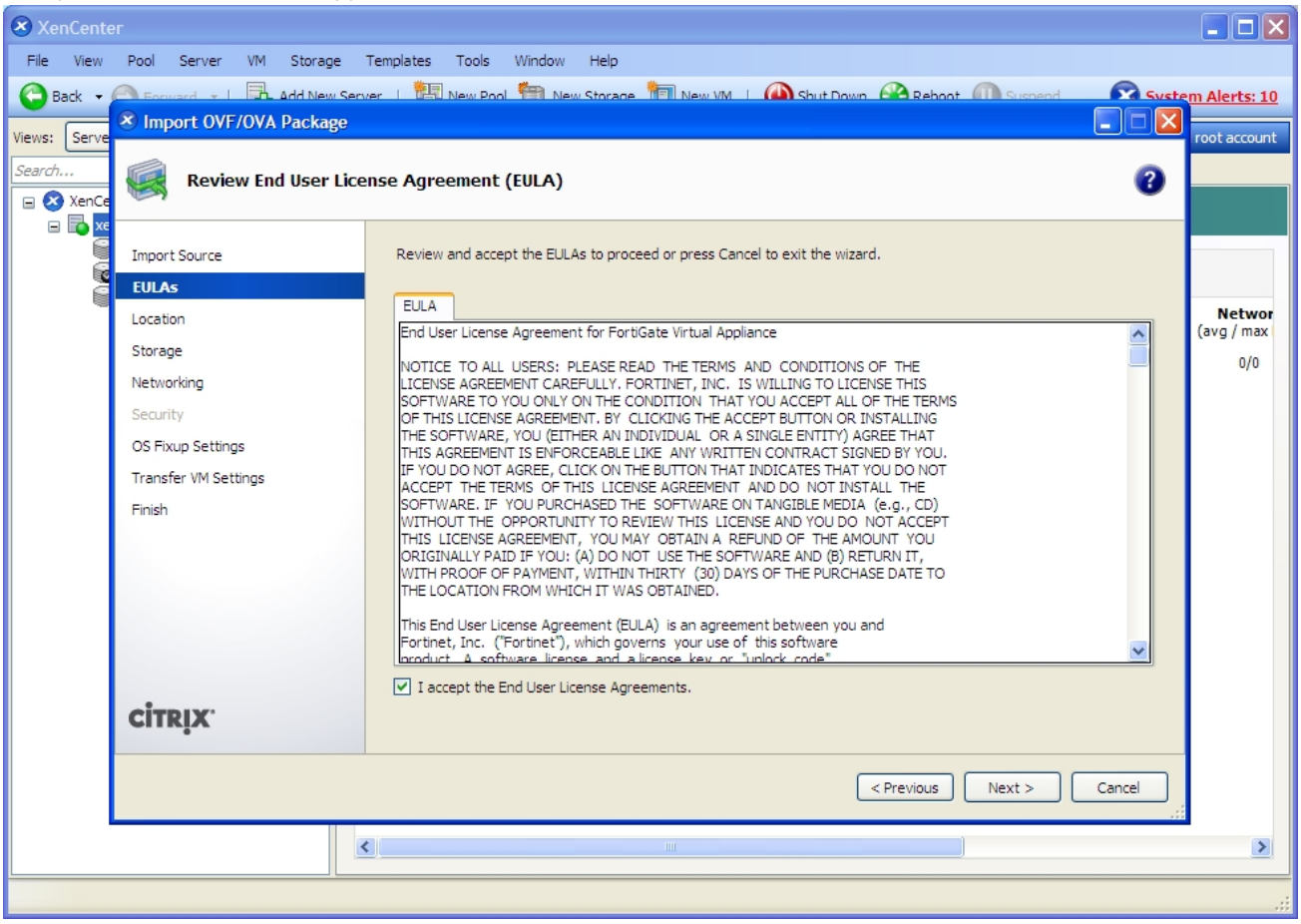
   The **Virtual Machine Manager** home page opens.
3. Go to **File > Import**. An import dialog will appear.

4. Click the **Browse** button, find the FortiGate-VM64-Xen.ovf template file, then click **Open**.



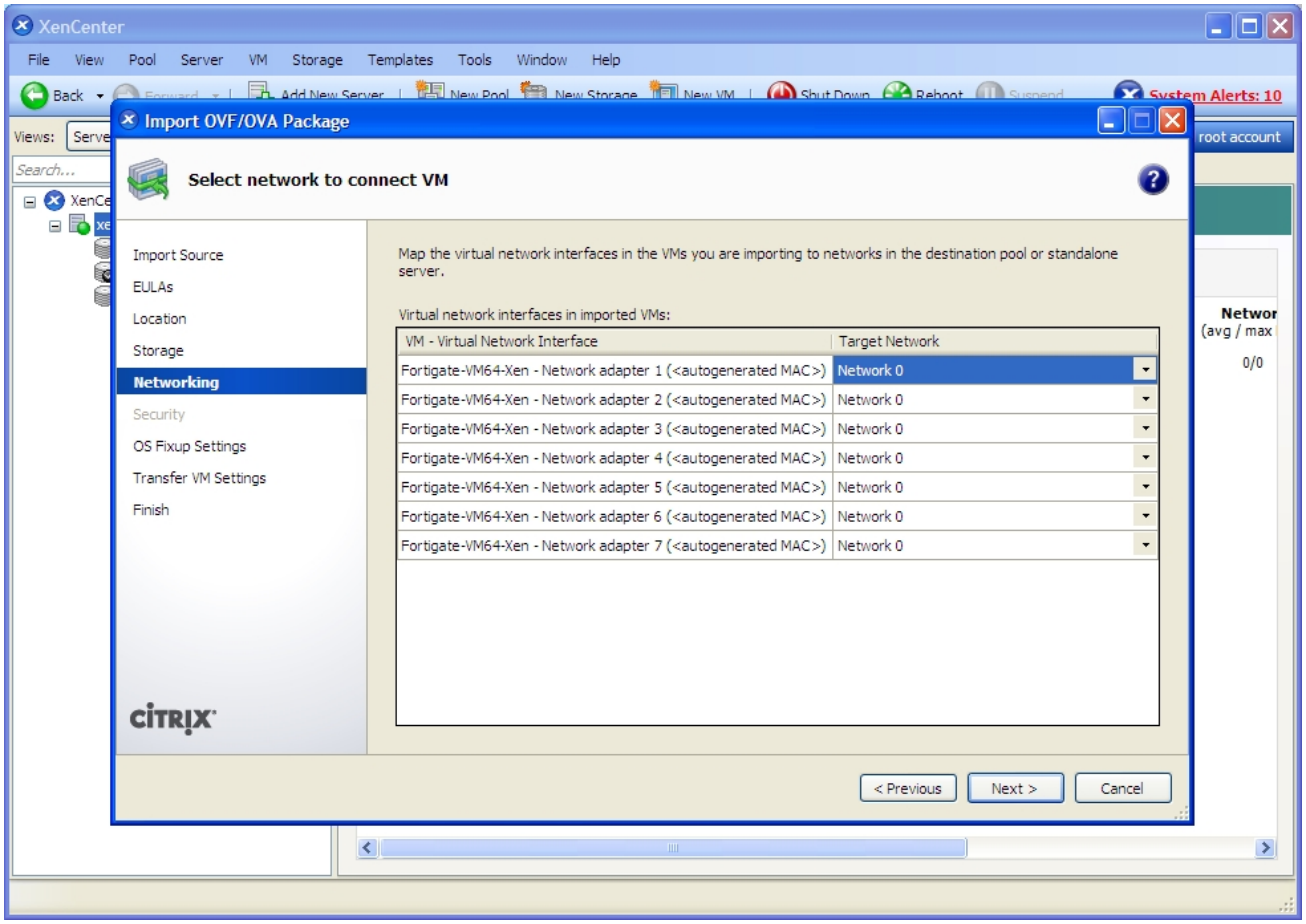
5. Select **Next**.

6. Accept the FortiGate Virtual Appliance EULA, then select **Next**.



7. Choose the pool or standalone server that will host the VM, then select **Next**.
8. Select the storage location for FortiGate VM disk drives or accept the default. Select **Next**.

9. Configure how each vNIC (virtual network adapter) in FortiGate VM will be mapped to each vNetwork on the Citrix XenServer, then click **Next**.



10. Click **Next** to skip OS fixup.
11. Select **Next** to use the default network settings for transferring the VM to the host.
12. Select **Finish**.

The Citrix XenServer imports the FortiGate VM files and configures the VM as specified in the OVF template. Depending on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, this might take several minutes to complete.

When VM import is complete, the XenCenter left pane includes the FortiGate VM in the list of deployed VMs for your Citrix XenServer.

Configure virtual hardware

Before you start your FortiGate-VM for the first time, you need to adjust your virtual machine's virtual hardware settings to meet your network requirements.

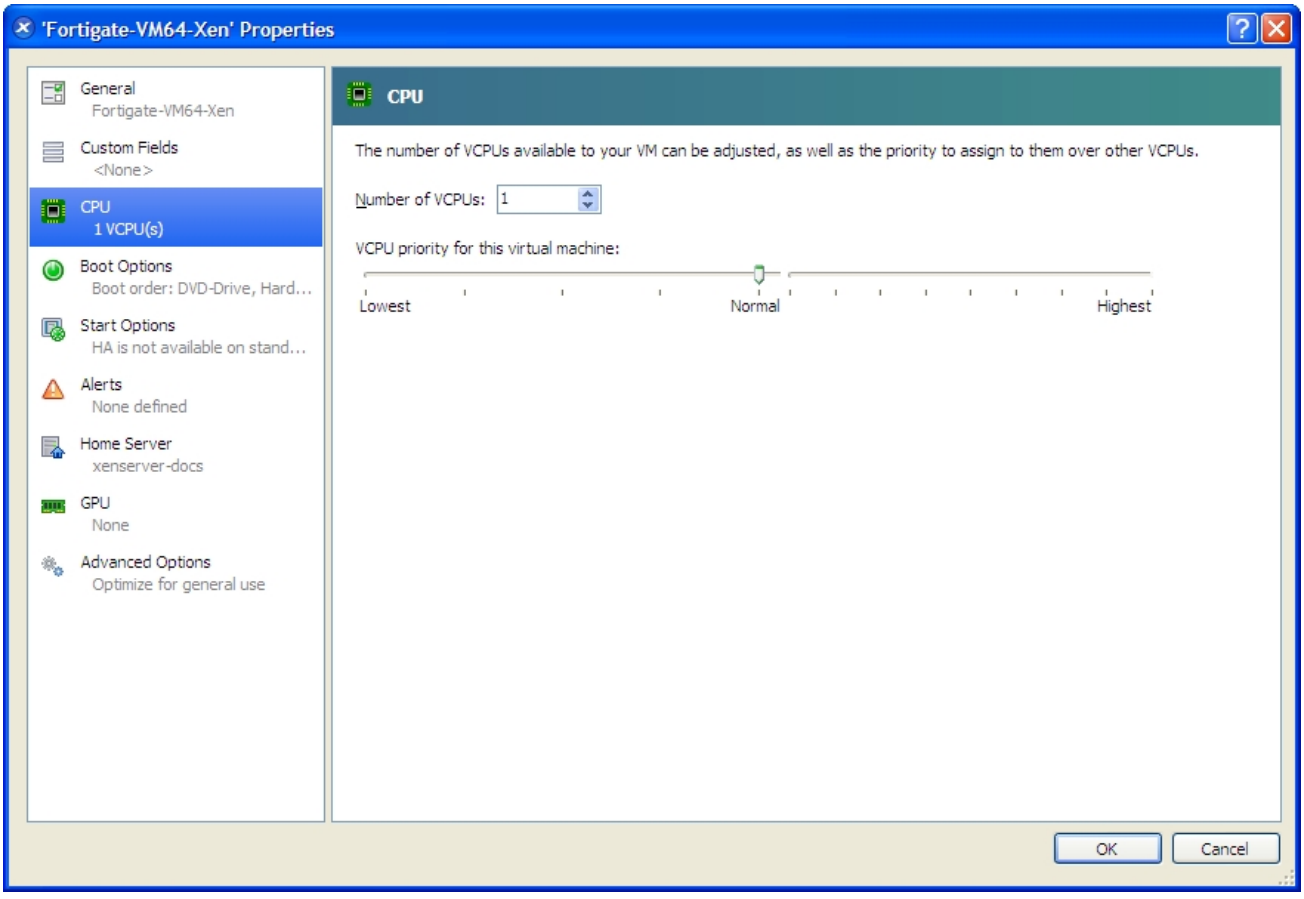
Configuring number of CPUs and memory size

Your FortiGate-VM license limits the number CPUs and amount of memory that you can use. The amounts you allocate must not exceed your license limits.

To access virtual machine settings

1. Open XenCenter.
2. Select your FortiGate VM in the left pane.
   The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiGate console.

1. To set the number of CPUs
2. In the XenCenter left pane, right-click the FortiGate VM and select Properties.
   The Properties window opens.
3. In the left pane, select CPU.

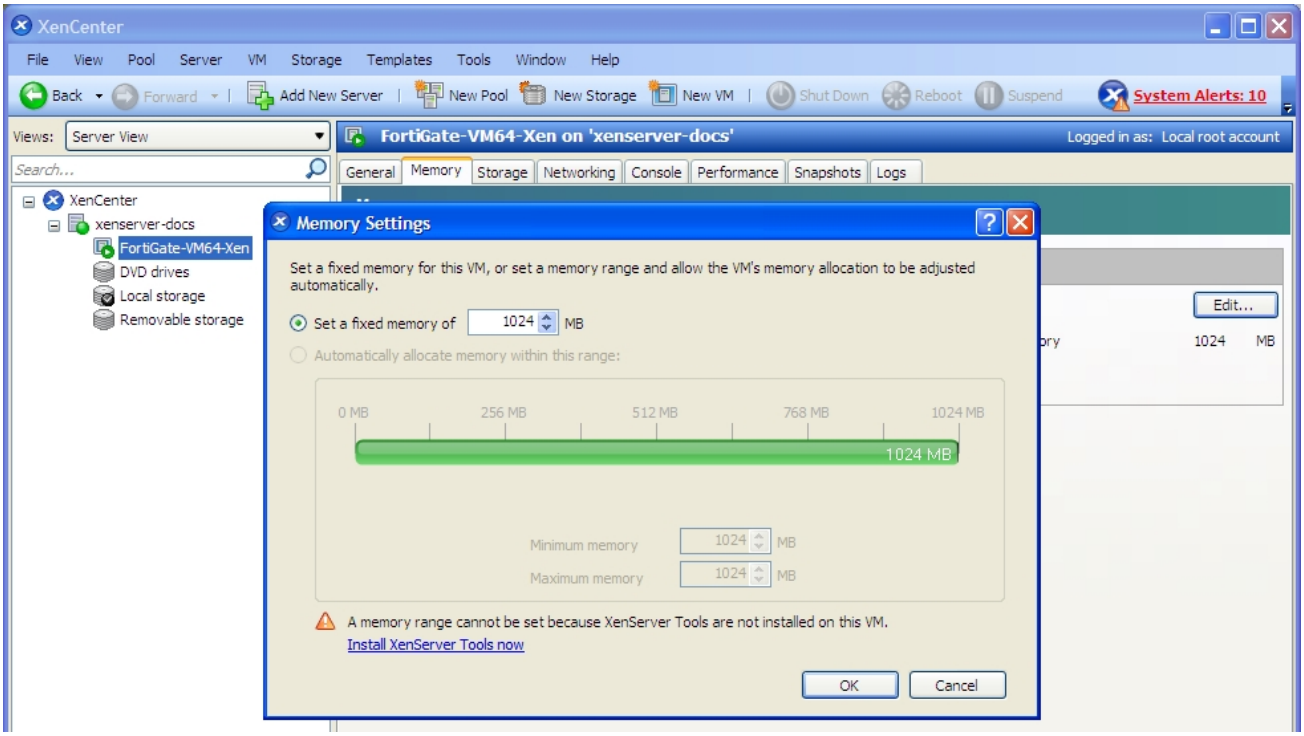


4. Adjust **Number of CPUs** and then select **OK**.

XenCenter will warn if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

To set memory size

1. In the XenCenter left pane, select the FortiGate VM.
2. In the right pane, select the **Memory** tab.
3. Select **Edit**, modify the value in the **Set a fixed memory of** field and select **OK**.



Configuring disk storage

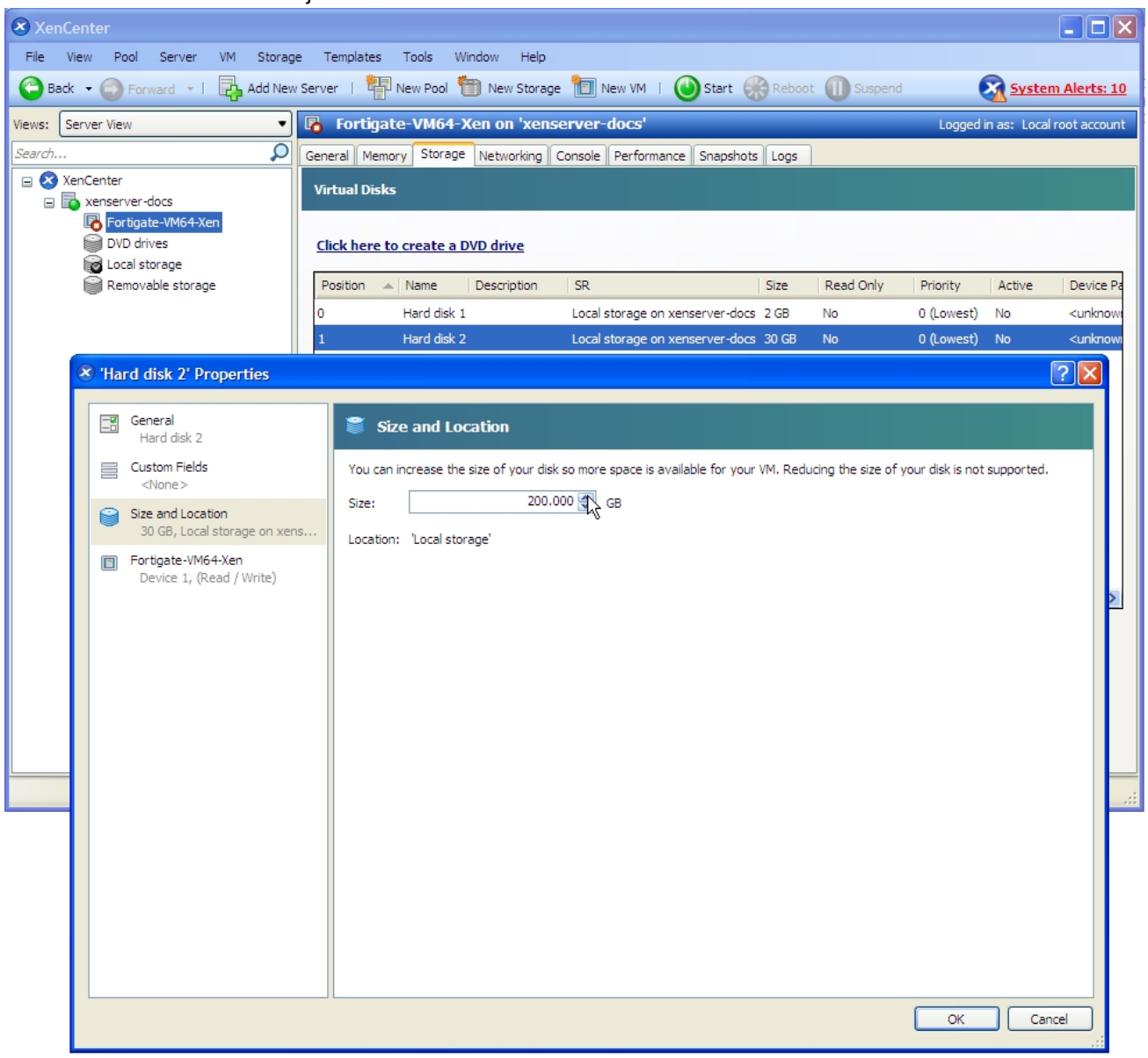
By default the FortiGate VM data disk 30GB. You will probably want to increase this. Disk resizing must be done before you start the VM for the first time.

To resize the FortiGate data disk

1. In the XenCenter left pane, select the FortiGate VM.
2. Select the **Storage** tab. Select **Hard disk 2** (the 30GB drive), then select **Properties**.

   The **'Hard disk 2' Properties** window opens.

3. Select **Size and Location**. Adjust **Size** and select **OK**.



FortiGate VM Initial Configuration

Before you can connect to the FortiGate VM web-based manager you must configure a network interface in the FortiGate VM console. Once an interface with administrative access is configured, you can connect to the FortiGate VM web-based Manager and upload the FortiGate VM license file that you downloaded from the Customer Service & Support website.

The following topics are included in this section:

Set FortiGate VM port1 IP address
Connect to the FortiGate VM Web-based Manager
Upload the FortiGate VM license file
Validate the FortiGate VM license with FortiManager
Configure your FortiGate VM

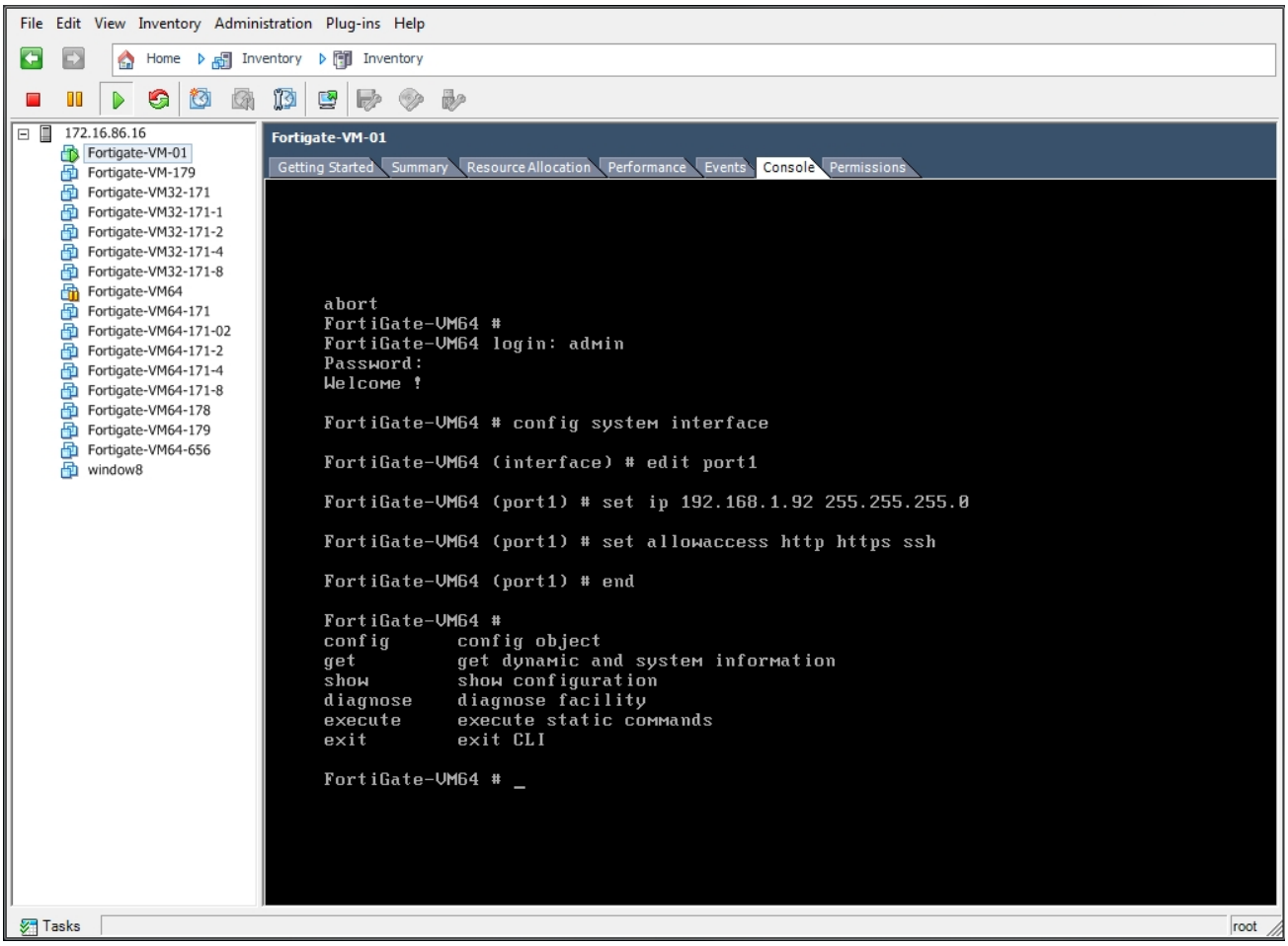
Set FortiGate VM port1 IP address

Hypervisor management environments include a guest console window. On the FortiGate VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the Web-based manager, you must configure FortiGate VM port1 with an IP address and administrative access.

To configure the port1 IP address:

1. In your hypervisor manager, start the FortiGate VM and access the console window.
   You might need to press Return to see a login prompt.

   Example of FortiGate VM console access:



2. At the FortiGate VM login prompt enter the username `admin`. By default there is no password. Just press Return.
3. Using CLI commands, configure the port1 IP address and netmask. Also, HTTP access must be enabled because until it is licensed the FortiGate VM supports only low-strength encryption. HTTPS access will not work.

   For example:

```
config system interface
   edit port1
      set ip 192.168.0.100 255.255.255.0
      append allowaccess http
   end
```

You can also use the `append allowaccess` CLI command to enable other access protocols, such as `auto-ipsec`, `http`, `probe-response`, `radius-acct`, `snmp`, and `telnet`. The `ping`, `https`, `ssh`, and `fgfm` protocols are enabled on the `port1` interface by default.

4. To configure the default gateway, enter the following CLI commands:

```
config router static
   edit 1
      set device port1
      set gateway <class_ip>
end
```

You must configure the default gateway with an IPv4 address. FortiGate VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
   set primary <Primary DNS server>
   set secondary <Secondary DNS server>
end
```

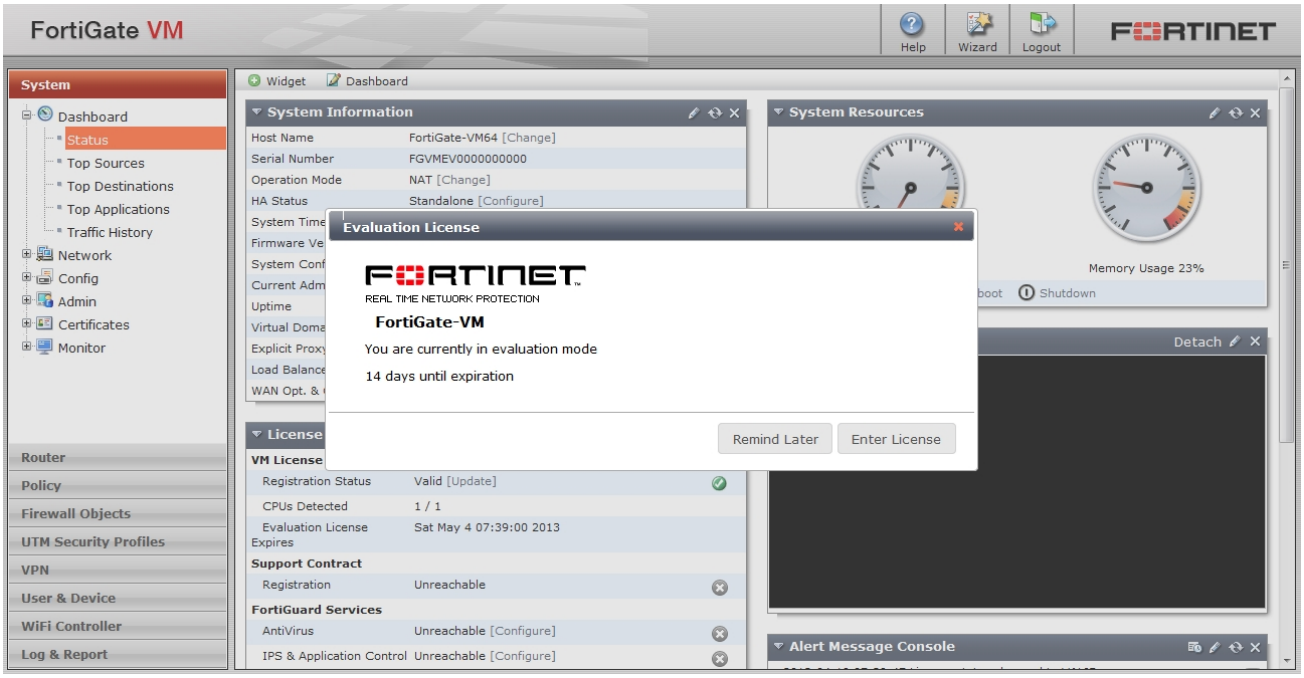
The default DNS servers are `208.91.112.53` and `208.91.112.52`.

6. To upload the FortiGate VM license from an FTP or TFTP server, use the following CLI command:

```
execute restore vmlicense {ftp | tftp} <VM license file name> <Server IP or FQDN>
    [:server port]
```

You can also upload the license in the FortiGate VM Web-based Manager. See Set FortiGate VM port1 IP address on page 2709.

Web-based Manager and Evaluation License dialog box



Connect to the FortiGate VM Web-based Manager

When you have configured the port1 IP address and netmask, launch a web browser and enter the IP address that you configured for port1. At the login page, enter the username `admin` and password field and select **Login**. The default password is no password. The Web-based Manager will appear with an **Evaluation License** dialog box.

Upload the FortiGate VM license file

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate VM operates in evaluation mode. Before using the FortiGate VM you must enter the license file that you downloaded from the Customer Service & Support website upon registration.

To upload the FortiGate VM licence file:

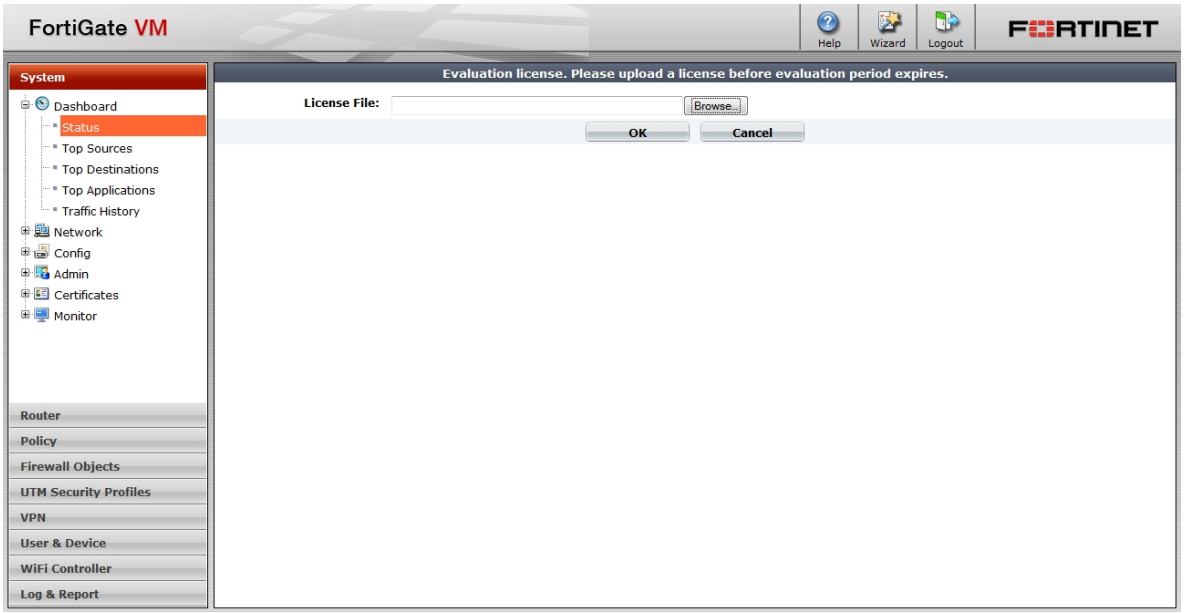
1. In the **Evaluation License** dialog box, select **Enter License**.

You can also upload the license file via the CLI using the following CLI command:

```
execute restore vmlicense [ftp | tftp] <filenmame string>
<ftp server>[:ftp port]
```

The license upload page opens.

License upload page:



2. Select **Browse** and locate the license file (`.lic`) on your computer. Select **OK** to upload the license file.
3. Refresh the browser to login.
4. Enter `admin` in the Name field and select **Login**. The VM registration status appears as valid in the License Information widget once the license has been validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.

Validate the FortiGate VM license with FortiManager

You can validate your FortiGate VM license with some models of FortiManager. To determine whether your FortiManager unit has the VM Activation feature, see Features section of the FortiManager Product Data sheet.

To validate your FortiGate VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:

```
config fmupdate publicnetwork
   set status disable
end
```

2. To configure FortiGate VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate VM:

```
config system central-management
   set mode normal
   set type fortimanager
   set include-default-servers disable
   set vdom <Enter the name of the VDOM to use when communicating with the FortiManager
       device>
   config server-list
      edit 1
         set server-type update rating
         set server-address <your FMG IP>
      next
   end
end
```

3. Load the FortiGate VM license file in the Web-based Manager.
   - Go to **System > Dashboard > Status**.
   - In the **License Information** widget, in the **Registration Status** field, select **Update**. Browse for the `.lic` license file and select **OK**.
4. To activate the FortiGate VM license, enter the following CLI command on your FortiGate VM:

```
execute update-now
```

5. To check the FortiGate VM license status, enter the following CLI commands on your FortiGate VM:

```
get system status
```

   The following output is displayed:

```
Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
```

```
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012

diagnose hardware sysinfo vm full
```

The following output is displayed:

```
UUID: 564db33a29519f6b1025bf8539a41e92
valid: 1
status: 1
code: 200 (If the license is a duplicate, code 401 will be displayed)
warn: 0
copy: 0
received: 45438
warning: 0
recv: 201201201918
dup:
```

Licensing timeout

In closed environments without Internet access, it is mandatory to perform offline licensing of the virtual FortiGate using a FortiManager as a license server. If the FortiGate-VM cannot perform license validation within the license timeout period, which is 30 days, the FortiGate will discard all packets and effectively ceasing operation as a firewall. There is only a single log entry after the virtual FortiGate cannot access the license server for the license expiration period.

Configure your FortiGate VM

Once the FortiGate VM license has been validated you can begin to configure your device. You can use the **Wizard** located in the top toolbar for basic configuration including enabling central management, setting the admin password, setting the time zone, and port configuration.

For more information on configuring your FortiGate VM see the FortiOS Handbook at http://docs.fortinet.com.

Chapter 29 - VoIP Solutions: SIP

This FortiOS Handbook chapter contains the following sections:

FortiGate VoIP solutions–SIP describes FortiGate SIP support.

FortiGate VoIP solutions–SIP

The Session Initiation Protocol (SIP) is an IETF application layer signaling protocol used for establishing, conducting, and terminating multiuser multimedia sessions over TCP/IP networks using any media. SIP is often used for Voice over IP (VoIP) calls but can be used for establishing streaming communication between end points.

SIP employs a request and response transaction model similar to HTTP for communicating between endpoints. SIP sessions being with a SIP client sending a SIP request message to another client to initiate a multimedia session. The other client responds with a SIP response message. Using these request and response messages, the clients engage in a SIP dialog to negotiate how to communicate and then start, maintain, and end the communication session.

SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with SSL or TLS.

Devices involved in SIP communications are called SIP User Agents (UAs) (also sometimes called a User Element (UE)). UAs include User Agent Clients (UACs) that communicate with each other and User Agent Servers (UASs) that facilitate communication between UACs. For a VoIP application, an example of a UAC would be a SIP phone and an example of a UAS would be a SIP proxy server.

A SIP message contain headers that include client and server names and addresses required for the communication sessions. The body of a SIP message contains Session Description Protocol (SDP) statements that establish the media communication (port numbers, protocols and codecs) that the SIP UAs use. SIP VoIP most commonly uses the Real Time Protocol (RTP) and the Real Time Control Protocol (RTCP) for voice communication. Once the SIP dialog establishes the SIP call the VoIP stream can run independently, although SIP messages can affect the VoIP stream by changing port numbers or addresses and by ending it.

Once SIP communication and media settings are established, the UAs communicate with each using the established media settings. When the communication session is completed, one of the UAs ends the session by sending a final SIP request message and the other UA sends a SIP response message and both UAs end the SIP call and stop the media stream.

FortiGate units provide security for SIP communications using the SIP session helper and the SIP ALG:

- The SIP session-helper provides basic high-performance support for SIP calls passing through the FortiGate unit by opening SIP and RTP pinholes and performing source and destination IP address and port translation for SIP and RTP packets and for the IP addresses and port numbers in the SIP headers and the SDP body of the SIP messages. For more about the SIP session helper, see The SIP session helper on page 2738.
- The SIP Application Layer Gateway (ALG) provides the same features as the session helper plus additional advanced features such as deep SIP message inspection, SIP logging, SIP IPv6 support, SIP message checking, HA failover of SIP sessions, and SIP rate limiting. For more about the SIP ALG, see The SIP ALG on page 2744.

All SIP traffic is processed by the SIP ALG by default. You can change the default setting using the following command:

```
config system settings
   set default-voip-alg-mode {proxy-based | kernel-helper-based}
end
```

The default is `proxy-based`, which means the SIP ALG is used. If set to `kernel-helper-based`, the SIP session helper is used. If a SIP session is accepted by a firewall policy with a VoIP profile, the session is processed using the SIP ALG even if `default-voip-alg-mode` is set to `kernel-helper-based`.

If a SIP session is accepted by a firewall policy that does not include a VoIP profile:

- If `default-voip-alg-mode` is set to `proxy-based`, SIP traffic is processed by the SIP ALG using the default VoIP profile.
- If `default-voip-alg-mode` is set to `kernel-helper-based`, SIP traffic is processed by the SIP session helper. If the SIP session help has been removed, then no SIP processing takes place.

On a FortiGate unit with multiple VDOMs, whether to use the ALG or the session helper is set per-VDOM.

There are a large number of SIP-related Internet Engineering Task Force (IETF) documents (Request for Comments) that define behavior of SIP and related applications. FortiGate units provide complete support of RFC 3261 for SIP, RFC 4566 for SDP and RFC 3262 for Provisional Response Acknowledgment (PRACK). FortiGate units also provide support for other SIP and SIP-related RFCs and performs Deep SIP message inspection on page 2792 for SIP statements defined in other SIP RFCs.

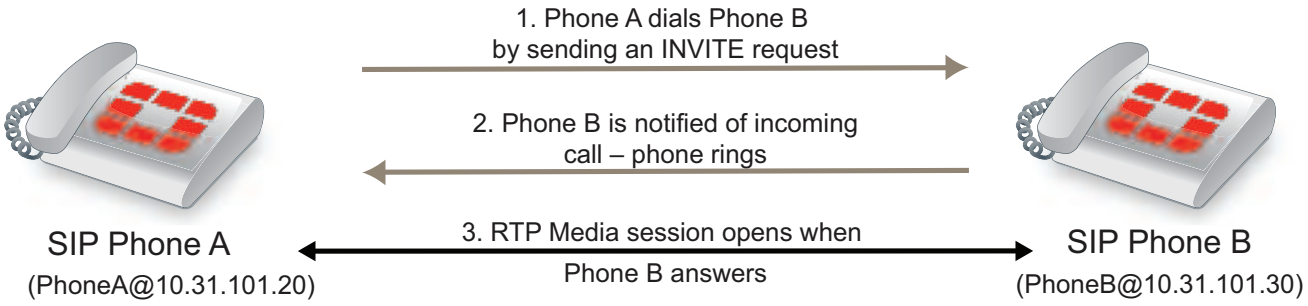
Common SIP VoIP configurations

This section describes some common SIP VoIP configurations and simplified SIP dialogs for these configurations. This section also shows some examples of how adding a FortiGate unit affects SIP processing.

Peer to peer configuration

In the peer to peer configuration shown below, two SIP phones (in the example, FortiFones) communicate directly with each other. The phones send SIP request and response messages back and forth between each other to establish the SIP session.

SIP peer to peer configuration

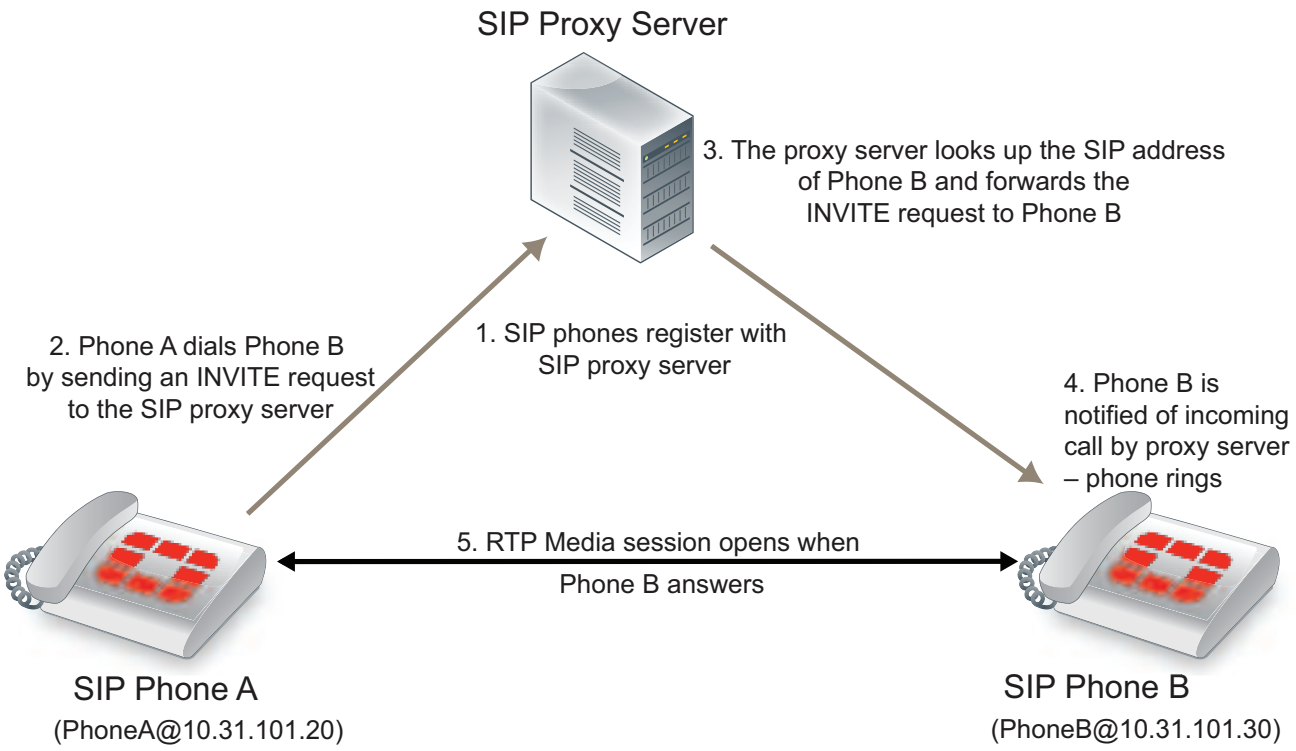


Peer to peer configurations are not very common because they require the SIP phones to keep track of the names and addresses of all of the other SIP phones that they can communicate with. In most cases a SIP proxy or re-direct server maintains addresses of a large number of SIP phones and a SIP phone starts a call by contacting the SIP proxy server.

SIP proxy server configuration

A SIP proxy server act as intermediary between SIP phones and between SIP phones (for example, two FortiFones) and other SIP servers. As shown below, SIP phones send request and response messages the SIP proxy server. The proxy server forwards the messages to other clients or to other SIP proxy servers. Proxy servers can hide SIP phones by proxying the signaling messages. To the other users on the VoIP network, the signaling invitations look as if they come from the SIP proxy server.

SIP in proxy mode

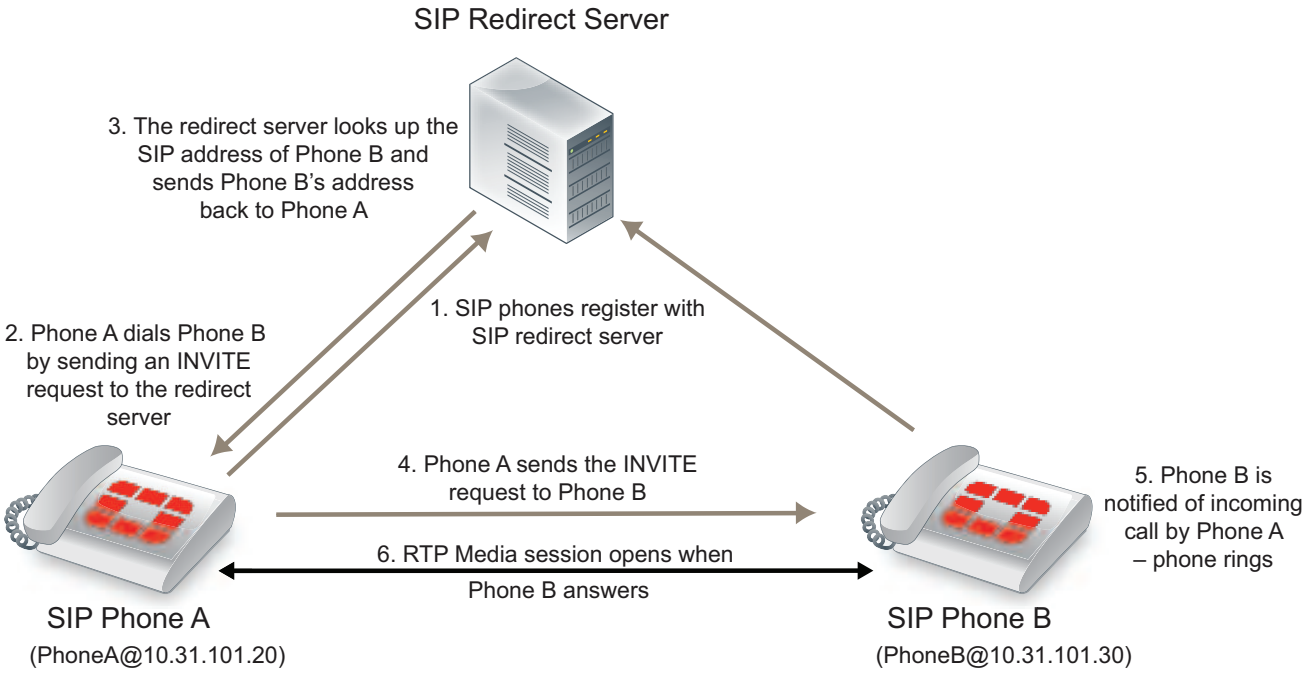


A common SIP configuration would include multiple networks of SIP phones. Each of the networks would have its own SIP server. Each SIP server would proxy the communication between phones on its own network and between phones in different networks.

SIP redirect server configuration

A SIP redirect server accepts SIP requests, maps the addresses in the request into zero or more new addresses and returns those addresses to the client. The redirect server does not initiate SIP requests or accept calls. As shown below, SIP clients send INVITE requests to the redirect server, which then looks up the destination address. The redirect server returns the destination address to the client. The client uses this address to send the INVITE request directly to the destination SIP client.

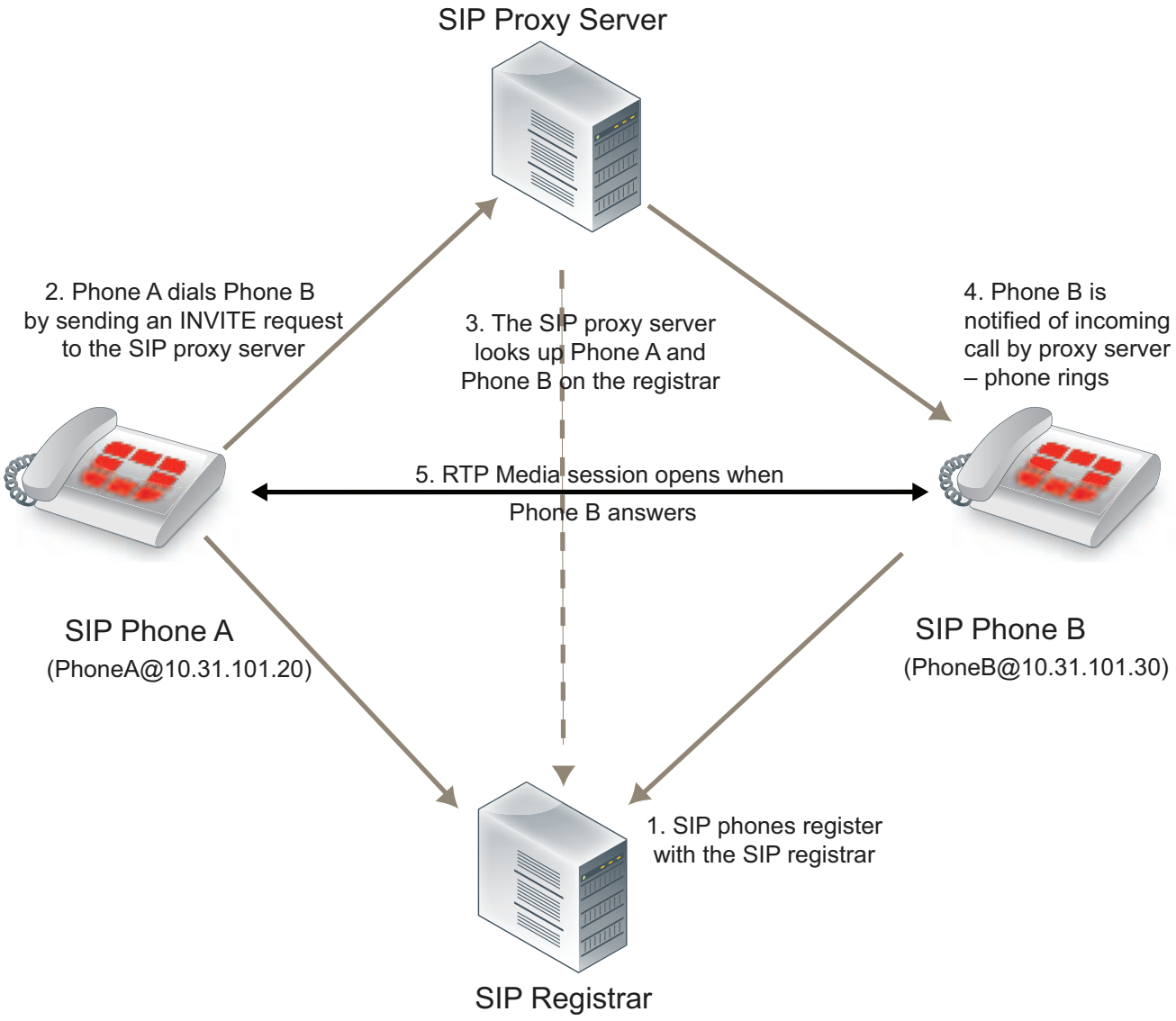
SIP in redirect model



SIP registrar configuration

A SIP registrar accepts SIP REGISTER requests from SIP phones for the purpose of updating a location database with this contact information. This database can then become a SIP location service that can be used by SIP proxy severs and redirect servers to locate SIP clients. As shown below, SIP clients send REGISTER requests to the SIP registrar.

SIP registrar and proxy servers

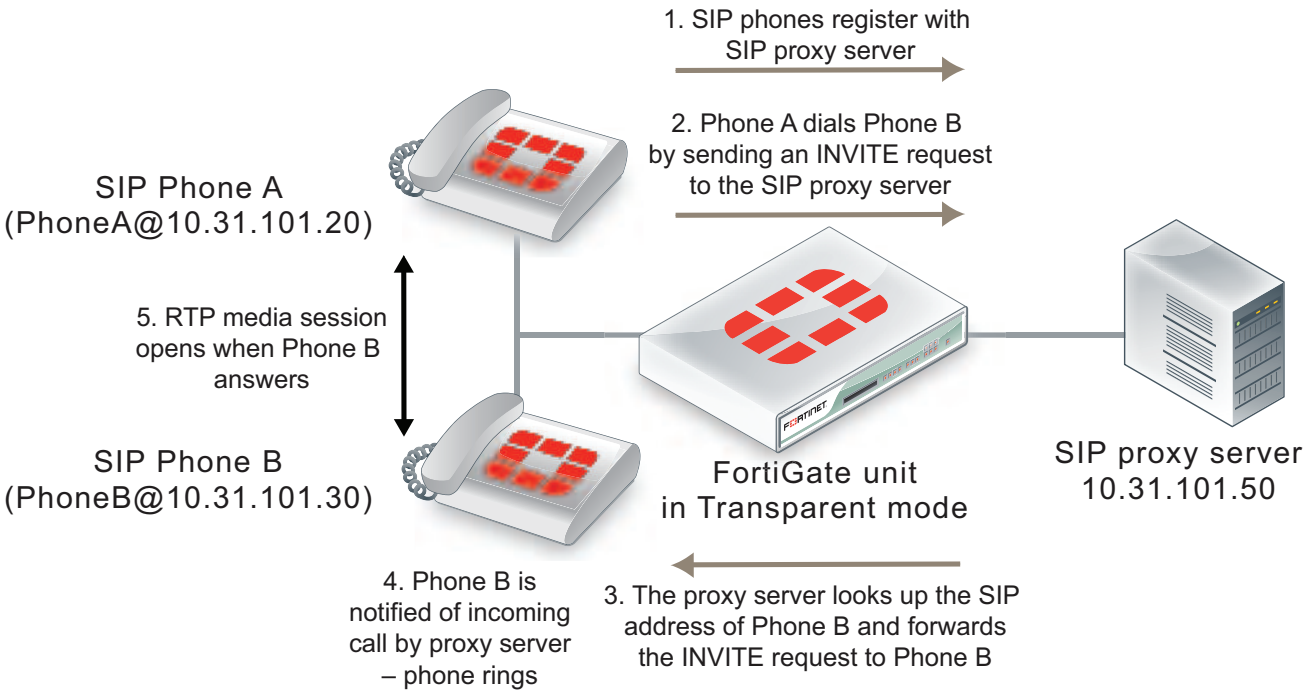


SIP with a FortiGate unit

Depending on your security requirements and network configuration FortiGate units may be in many different places in a SIP configuration. This section shows a few examples.

The diagram below shows a FortiGate unit installed between a SIP proxy server and SIP phones on the same network. The FortiGate unit is operating in Transparent mode so both the proxy server and the phones are on the same subnet. In this configuration, called SIP inspection without address translation, the FortiGate unit could be protecting the SIP proxy server on the private network by implementing SIP security features for SIP sessions between the SIP phones and the SIP proxy server.

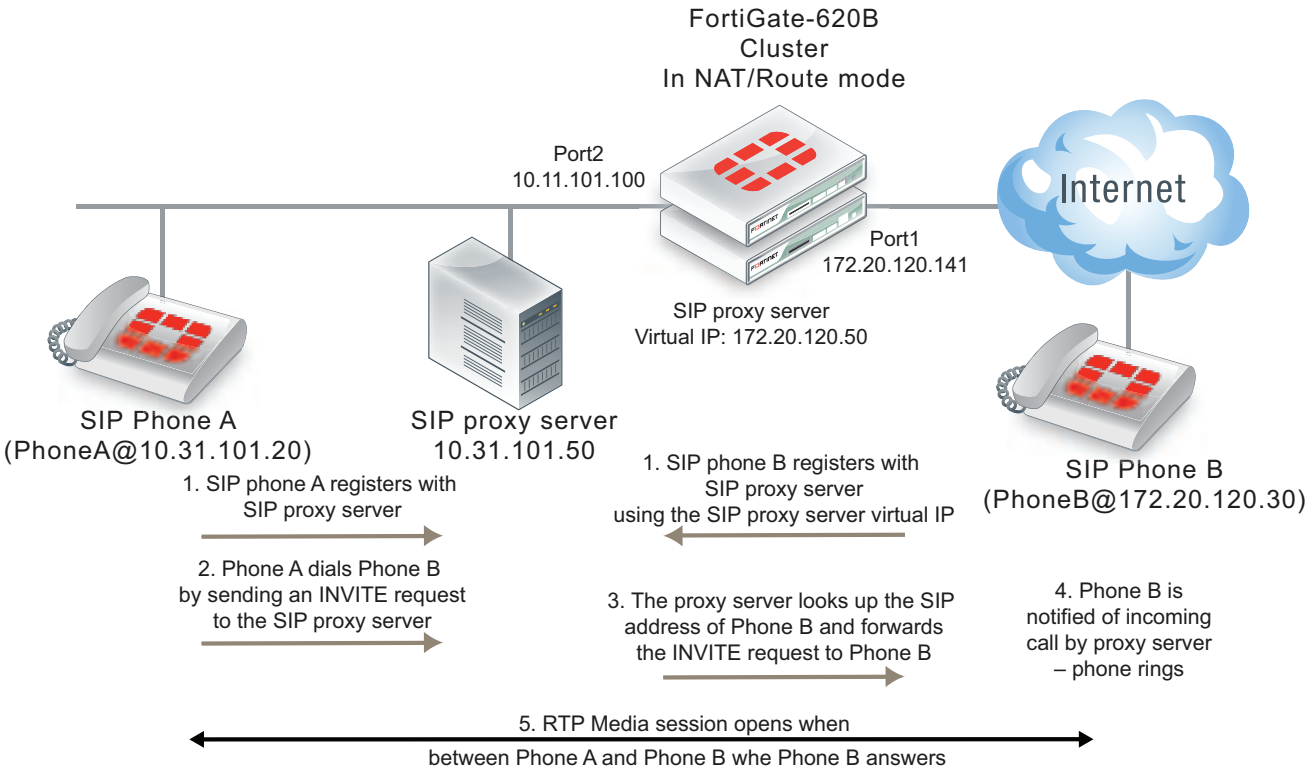
SIP network with FortiGate unit in Transparent mode



The phones and server use the same SIP dialogs as they would if the FortiGate unit was not present. However, the FortiGate unit can be configured to control which devices on the network can connect to the SIP proxy server and can also protect the SIP proxy server from SIP vulnerabilities.

The following diagram shows a FortiGate unit operating in NAT/Route mode and installed between a private network and the Internet. Some SIP phones and the SIP proxy server are connected to the private network and some SIP phones are connected to the Internet. The SIP phones on the Internet can connect to the SIP proxy server through the FortiGate unit and communication between SIP phones on the private network and SIP phones on the Internet must pass through the FortiGate unit.

SIP network with FortiGate unit in NAT/Route mode



The phones and server use the same SIP dialog as they would if the FortiGate unit was not present. However, the FortiGate unit can be configured to control which devices on the network can connect to the SIP proxy server and can also protect the SIP proxy server from SIP vulnerabilities. In addition, the FortiGate unit has a firewall virtual IP that forwards packets sent to the SIP proxy server Internet IP address (172.20.120.50) to the SIP proxy server internal network IP address (10.31.101.30).

Since the FortiGate unit is operating in NAT/Route mode it must translate packet source and destination IP addresses (and optionally ports) as the sessions pass through the FortiGate unit. Also, the FortiGate unit must translate the addresses contained in the SIP headers and SDP body of the SIP messages. As well the FortiGate unit must open SIP and RTP pinholes through the FortiGate unit. SIP pinholes allow SIP signalling sessions to pass through the FortiGate between phones and between phones and SIP servers. RTP pinholes allow direct RTP communication between the SIP phones once the SIP dialog has established the SIP call. Pinholes are opened automatically by the FortiGate unit. Administrators do not add security policies for pinholes or for RTP sessions. All that is required is a security policy that accepts SIP traffic.

Opening an RTP pinhole means opening a port on a FortiGate interface to allow RTP traffic to use that port to pass through the FortiGate unit between the SIP phones on the Internet and SIP phones on the internal network. A pinhole only accepts packets from one RTP session. Since a SIP call involves at least two media streams (one from Phone A to Phone B and one from Phone B to Phone A) the FortiGate unit opens two RTP pinholes. Phone A sends RTP packets through a pinhole in port2 and Phone B sends RTP packets through a pinhole in port1. The FortiGate unit opens the pinholes when required by the SIP dialog and closes the pinholes when the SIP call is completed. The FortiGate unit opens new pinholes for each SIP call.

Each RTP pinhole actually includes two port numbers. The RTP port number as defined in the SIP message and an RTCP port number, which is the RTP port number plus 1. For example, if the SIP call used RTP port 3346 the FortiGate unit would create a pinhole for ports 3346 and 3347.

SIP messages and media protocols

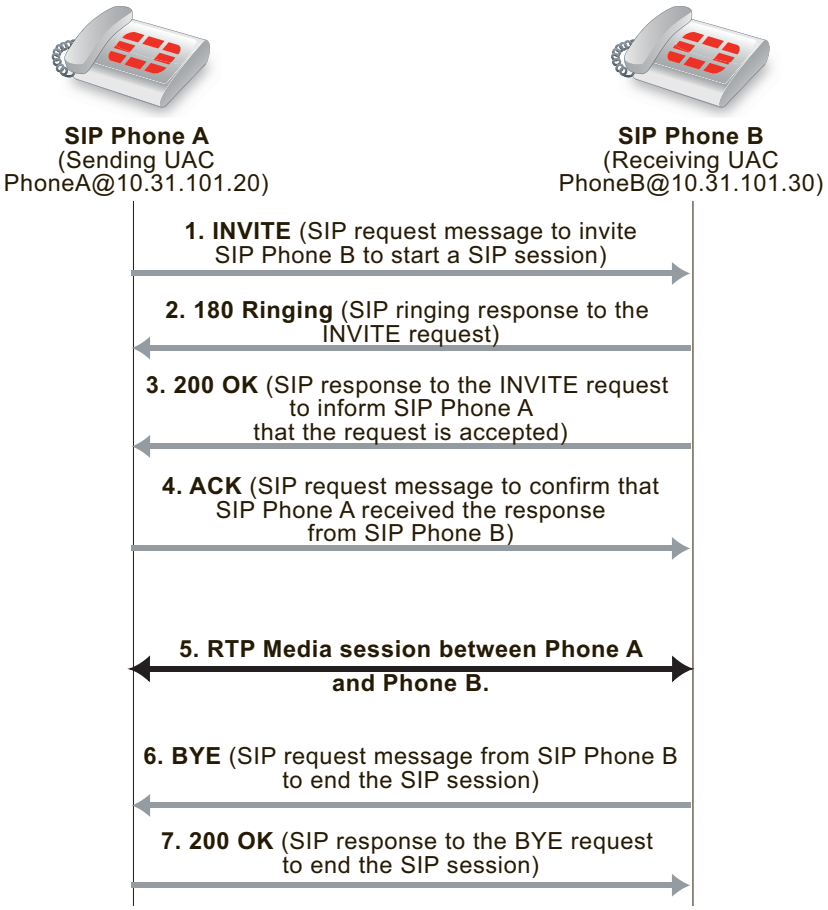
This section provides an overview of SIP messages and how they communicate information about SIP sessions and how SDP, RTP, and RTCP fits in with SIP communications.

SIP uses clear text messages to start, maintain, and end media sessions between SIP user agent clients (UACs) and user agent servers (UASs). These messages form a SIP dialog. A typical SIP dialog begins with an INVITE request message sent from a UAC to another UAC or to a UAS. The first INVITE request message attempts to start a SIP call and includes information about the sending UAC and the receiving UAC as well as information about the communication session.

If only two UACs are involved as shown below, the receiving UAC (Phone B) responds with a 180 Ringing and then a 200 OK SIP response message that informs Phone A that Phone B received and accepted the request. Phone A then sends an ACK message to notify Phone B that the SIP response was received. Phone A and Phone B can then participate in the RTP media session set up by the SIP messages.

When the phone call is complete, one of the UACs (in the example Phone B) hangs up sending a BYE request message to Phone A. Phone A then sends a 200 OK response to Phone B acknowledging that the session has ended.

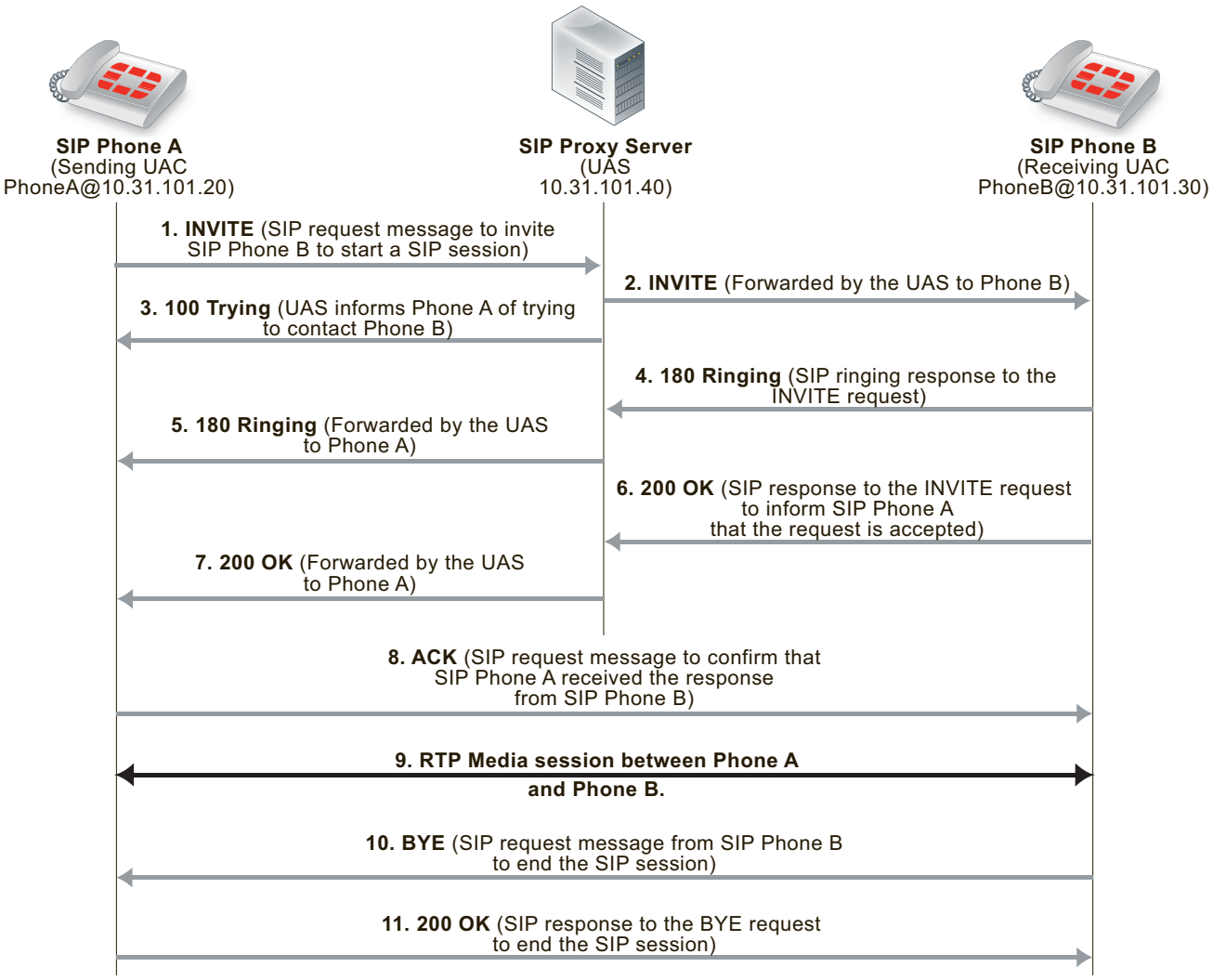
Basic SIP dialog between two UACs



If a UAS in the form of a SIP proxy server is involved, similar messages are sent and received, but the proxy server participates as an intermediary in the initial call setup. In the example below the SIP proxy server receives the INVITE request from Phone A and forwards it to Phone B. The proxy server then sends a 100 Trying response to Phone A. Phone B receives the INVITE request and responds with a 180 Ringing and then a 200 OK SIP response message. These messages are received by the proxy server and forwarded to Phone A to notify Phone A that Phone B received and accepted the request. Phone A then sends an ACK message to notify Phone B that the SIP response was received. This response is received by the proxy server and forwarded to Phone B. Phone A and Phone B can then participate in the media session independently of the proxy server.

When the phone call is complete Phone B hangs up sending a BYE request message to Phone A. Phone A then sends a 200 OK response to Phone B acknowledging that the session has ended.

Basic SIP dialog between UACs with a SIP proxy server UAS



The SIP messages include SIP headers that contain names and addresses of Phone A, Phone B and the proxy server. This addressing information is used by the UACs and the proxy server during the call set up.

The SIP message body includes Session Description Protocol (SDP) statements that Phone A and Phone B use to establish the media session. The SDP statements specify the type of media stream to use for the session (for example, audio for SIP phone calls) and the protocol to use for the media stream (usually the Real Time Protocol (RTP) media streaming protocol).

Phone A includes the media session settings that it would like to use for the session in the INVITE message. Phone B includes its response to these media settings in the 200 OK response. Phone A's ACK response confirms the settings that Phone A and Phone B then use for the media session.

Hardware accelerated RTP processing

FortiGate units can offload RTP packet processing to network processor (NP) interfaces. This acceleration greatly enhance the overall throughput and resulting in near speed RTP performance.

SIP request messages

SIP sessions always start with a SIP request message (also just called a SIP request). SIP request messages also establish, maintain, and terminate SIP communication sessions. The following table lists some common SIP request message types.

Common SIP request message types

Message Type	Description
INVITE	A client sends an INVITE request to invite another client to participate in a multimedia session. The INVITE request body usually contains the description of the session.
ACK	The originator of an INVITE message sends an ACK request to confirm that the final response to an INVITE request was received. If the INVITE request did not contain the session description, it must be included in the ACK request.
PRACK	In some cases, SIP uses provisional response messages to report on the progress of the response to a SIP request message. The provisional response messages are sent before the final SIP response message. Similar to an ACK request message, a PRACK request message is sent to acknowledge that a provisional response message has been received.
OPTIONS	The UA uses OPTIONS messages to get information about the capabilities of a SIP proxy. The SIP proxy server replies with a description of the SIP methods, session description protocols, and message encoding that are supported.
BYE	A client sends a BYE request to end a session. A BYE request from either end of the SIP session terminates the session.
CANCEL	A client sends a CANCEL request to cancel a previous INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE sends a final response to the INVITE before receiving the CANCEL.
REGISTER	A client sends a REGISTER request to a SIP registrar server with information about the current location (IP address and so on) of the client. A SIP registrar server saves the information it receives in REGISTER requests and makes this information available to any SIP client or server attempting to locate the client.
Info	For distributing mid-session signaling information along the signaling path for a SIP call. I
Subscribe	For requesting the current state and state updates of a remote node.
Notify	Informs clients and servers of changes in state in the SIP network.
Refer	Refers the recipient (identified by the Request-URI) to a third party according to the contact information in the request.
Update	Opens a pinhole for new or updated SDP information.
Response codes (1xx, 202, 2xx, 3xx, 4xx, 5xx, 6xx)	Indicates the status of a transaction. For example: 200 OK, 202 Accepted, or 400 Bad Request.

SIP response messages

SIP response messages (often just called SIP responses) provide status information in response to SIP request messages. All SIP response messages include a response code and a reason phrase. There are five SIP response message classes. They are described below.

There are also two types of SIP response messages, provisional and final. Final response messages convey the result of the request processing, and are sent reliably. Provisional responses provide information on the progress of the request processing, but may not be sent reliably. Provisional response messages start with 1xx and are also called informational response messages.

Informational (or provisional)

Informational or provisional responses indicate that a request message was received and imply that the endpoint is going to process the request. Information messages may not be sent reliably and may not require an acknowledgement.

If the SIP implementation uses Provisional Response Acknowledgement (PRACK) (RFC 3262) then informational or provisional messages are sent reliably and require a PRACK message to acknowledge that they have been received.

Informational responses can contain the following reason codes and reason phrases:

```
100 Trying
180 Ringing
181 Call is being forwarded
182 Queued
183 Session progress
```

Success

Success responses indicate that a request message was received, understood, and accepted. Success responses can contain the following reason codes and reason phrases:

```
200 OK
202 Accepted
```

Redirection

Redirection responses indicate that more information is required for the endpoint to respond to a request message. Redirection responses can contain the following reason codes and reason phrases:

```
300 Multiple choices
301 Moved permanently
302 Moved temporarily
305 Use proxy
380 Alternative service
```

Client error

Client error responses indicate that a request message was received by a server that contains syntax that the server cannot understand (i.e. contains a syntax error) or cannot comply with. Client error responses include the following reason codes and reason phrases:

```
400 Bad request              401 Unauthorized
```

```
402 Payment required          403 Forbidden
404 Not found                 405 Method not allowed
406 Not acceptable            407 Proxy authentication required
408 Request time-out          409 Conflict
410 Gone                      411 Length required
413 Request entity too large  414 Request-URL too large
415 Unsupported media type    420 Bad extension
480 Temporarily not available
481 Call leg/transaction does not exist
482 Loop detected
484 Address incomplete        483 Too many hops
486 Busy here                 485 Ambiguous
488 Not acceptable here       487 Request canceled
```

Server error

Server error responses indicate that a server was unable to respond to a valid request message. Server error responses include the following reason codes and reason phrases:

```
500 Server internal error
501 Not implemented
502 Bad gateway
502 Service unavailable
504 Gateway time-out
505 SIP version not supported
```

Global failure

Global failure responses indicate that there are no servers available that can respond to a request message. Global failure responses include the following reason codes and reason phrases:

```
600 Busy everywhere
603 Decline
604 Does not exist anywhere
606 Not acceptable
```

SIP message start line

The first line in a SIP message is called the start line. The start line in a request message is called the request-line and the start line in a response message is called the status-line.

Request-line	The first line of a SIP request message. The request-line includes the SIP message type, the SIP protocol version, and a Request URI that indicates the user or service to which this request is being addressed. The following example request-line specifies the INVITE message type, the address of the sender of the message (`inviter-@example.com`), and the SIP version: `INVITE sip:inviter@example.com SIP/2.0`
Status-line	The first line of a SIP response message. The status-line includes the SIP protocol version, the response code, and the reason phrase. The example status-line includes the SIP version, the response code (`200`) and the reason phrase (`OK`). `SIP/2.0 200 OK`

SIP headers

Following the start line, SIP messages contain SIP headers (also called SIP fields) that convey message attributes and to modify message meaning. SIP headers are similar to HTTP header fields and always have the following format:

```
<header_name>:<value>
```

SIP messages can include the SIP headers listed in the following table:

SIP headers

SIP Header	Description
Allow	Lists the set of SIP methods supported by the UA generating the message. All methods, including ACK and CANCEL, understood by the UA MUST be included in the list of methods in the Allow header field, when present. For example: `Allow: INVITE, ACK, OPTIONS, CANCEL, BYE`
Call-ID	A globally unique identifier for the call, generated by the combination of a random string and the sender's host name or IP address. The combination of the To, From, and Call-ID headers completely defines a peer-to-peer SIP relationship between the sender and the receiver. This relationship is called a SIP dialog. `Call-ID: ddeg45e793@10.31.101.30`
Contact	Included in SIP request messages, the Contact header contains the SIP URI of the sender of the SIP request message. The receiver uses this URI to contact the sender. For example: `Contact: Sender <sip:sender@10.31.100.20>t`
Content-Length	The number of bytes in the message body (in bytes). `Content-Length: 126`
Content-Type	In addition to SIP headers, SIP messages include a message body that contains information about the content or communication being managed by the SIP session. The Content-Type header specifies what the content of the SIP message is. For example, if you are using SIP with SDP, the content of the SIP message is SDP code. `Content-Type: application/sdp`
CSeq	The command sequence header contains a sequence integer that is increased for each new SIP request message (but is not incremented in the response message). This header also incudes the request name found in the request message request-line. For example: `CSeq: 1 INVITE`
Expires	Gives the relative time after which the message (or content) expires. The actual time and how the header is used depends on the SIP method. For example: `Expires: 5`
From	Identifies the sender of the message. Responses to a message are sent to the address of the sender. The following example includes the sender's name (`Sender`) and the sender's SIP address (`sender@10.31.101.20.`): `From: Sender <sip:sender@10.31.101.20>`

SIP Header	Description
Max-forwards	An integer in the range 0-255 that limits the number of proxies or gateways that can forward the request message to the next downstream server. Also called the number of hops, this value is decreased every time the message is forwarded. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain. `For example: Max-Forwards: 30`
P-Asserted-Identity	The P-Asserted-Identity header is used among trusted SIP entities to carry the identity of the user sending a SIP message as it was verified by authentication. See RFC 3325. The header contains a SIP URI and an optional display-name, for example: `P-Asserted-Identity: "Example Person" <sip:10.31.101.50>`
RAck	Sent in a PRACK request to support reliability of information or provisional response messages. It contains two numbers and a method tag. For example: `RAck: 776656 1 INVITE`
Record-Route	Inserted into request messages by a SIP proxy to force future requests to be routed through the proxy. In the following example, the host at IP address 10.31.101.50 is a SIP proxy. The `lr` parameter indicates the URI of a SIP proxy in Record-Route headers. `Record-Route: <sip:10.31.101.50;lr>`
Route	Forces routing for a request message through one or more SIP proxies. The following example includes two SIP proxies: `Route: <sip:172.20.120.10;lr>, <sip:10.31.101.50;lr>`
RSeq	The RSeq header is used in information or provisional response messages to support reliability of informational response messages. The header contains a single numeric value. For example: `RSeq: 33456`
To	Identifies the receiver of the message. The address in this field is used to send the message to the receiver. The following example includes the receiver's name (`Receiver`) and the receiver's SIP address (`receiver@10.31.101.30`.): `To: Receiver <sip:receiver@10.31.101.30>`
Via	Indicates the SIP version and protocol to be used for the SIP session and the address to which to send the response to the message that contains the Via field. The following example Via field indicates to use SIP version 2, UDP for media communications, and to send the response to 10.31.101.20 using port 5060. `Via: SIP/2.0/UDP 10.31.101.20:5060`

The SIP message body and SDP session profiles

The SIP message body describes the session to be initiated. For example, in a SIP phone call the body usually includes audio codec types, sampling rates, server IP addresses and so on. For other types of SIP session the body could contain text or binary data of any type which relates in some way to the session. The message body is included in request and response messages.

Two possible SIP message body types:

- Session Description Protocol (SDP), most commonly used for SIP VoIP.
- Multipurpose Internet Mail Extensions (MIME)

SDP is most often used for VoIP and FortiGate units support SDP content in SIP message bodies. SDP is a text-based protocol used by SIP to control media sessions. SDP does not deliver media but provides a session profile that contains media details, transport addresses, parameter negotiation, and other session description metadata for the participants in a media session. The participants use the information in the session profile to negotiate how to communicate and to manage the media session. SDP is described by RFC 4566.

An SDP session profile always contains session information and may contain media information. Session information appears at the start of the session profile and media information (using the `m=` attribute) follows.

SDP session profiles can include the attributes listed inthe following table.

SDP session profile attributes

Attribute	Description
a=	Attributes to extend SDP in the form `a=<attribute>` or `a=<attribute>:<value>`.
b=	Contains information about the bandwidth required for the session or media in the form `b=<bandwidth_type>:<bandwidth>`.
c=	Connection data about the session including the network type (usually IN for Internet), address type (IPv4 or IPv6), the connection source address, and other optional information. For example: `c=IN IPv4 10.31.101.20`
i=	A text string that contains information about the session. For example: `i=A audio presentation about SIP`
k=	Can be used to convey encryption keys over a secure and trusted channel. For example: `k=clear:444gdduudjffdee`

m=	Media information, consisting of one or more lines all starting with `m=` and containing details about the media including the media type, the destination port or ports used by the media, the protocol used by the media, and a media format description.
	
	`m=audio 49170 RTP 0 3`
	`m-video 3345/2 udp 34`
	`m-video 2910/2 RTP/AVP 3 56`
	
	Multiple media lines are needed if SIP is managing multiple types of media in one session (for example, separate audio and video streams).
	
	Multiple ports for a media stream are indicated using a slash. `3345/2` udp means UDP ports 3345 and 3346. Usually RTP uses even-numbered ports for data with the corresponding one-higher odd ports used for the RTCP session belonging to the RTP session. So `2910/2 RTP/AVP` means ports 2910 and 2912 are used for RTP and 2911 and 2913 are used for RTCP.
	
	Media types include `udp` for an unspecified protocol that uses UDP, `RTP` or `RTP/AVP` for standard RTP and `RTP/SAVP` for secure RTP.

o=	The sender's username, a session identifier, a session version number, the network type (usually IN for Internet), the address type (for example, IPv4 or IPv6), and the sending device's IP address. The `o=` field becomes a universal identifier for this version of this session description. For example: `o=PhoneA 5462346 332134 IN IP4 10.31.101.20`

Attribute	Description
r=	Repeat times for a session. Used if a session will be repeated at one or more timed intervals. Not normally used for VoIP calls. The times can be in different formats. For example: `r=7d 1h 0 25h r=604800 3600 0 90000`
s=	Any text that describes the session or s= followed by a space. For example: `s=Call from inviter`
t=	The start and stop time of the session. Sessions with no time restrictions (most VoIP calls) have a start and stop time of 0. `t=0 0`
v=	SDP protocol version. The current SDP version is 0 so the v= field is always: `v=0`
z=	Time zone adjustments. Used for scheduling repeated sessions that span the time between changing from standard to daylight savings time. `z=2882844526 -1h 2898848070 0`

Example SIP messages

The following example SIP INVITE request message was sent by PhoneA to PhoneB. The first nine lines are the SIP headers. The SDP profile starts with v=0 and the media part of the session profile is the last line, starting with m=.

```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
Content-Type: application/sdp
Content-Length: 124
v=0
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
s=Let's Talk
t=0 0
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
```

The following example shows a possible 200 OK SIP response message in response to the previous INVITE request message. The response includes `200 OK` which indicates success, followed by an echo of the original SIP INVITE request followed by PhoneB's SDP profile.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.31.101.50:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
```

```
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneB@10.31.101.30
Content-Type: application/sdp
Content-Length: 107
v=0
o=PhoneB 124333 67895 IN IP4 172.20.120.30
s=Hello!
t=0 0
c=IN IP4 172.20.120.30
m=audio 3456 RTP 0
```

SIP can support multiple media streams for a single SIP session. Each media steam will have its own c= and m= lines in the body of the message. For example, the following message includes three media streams:

```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
Content-Type: application/sdp
Content-Length: 124
v=0
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
s=Let's Talk
t=0 0
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
c=IN IP4 10.31.101.20
m=audio 49172 RTP 0 3
c=IN IP4 10.31.101.20
m=audio 49174 RTP 0 3
```

The SIP session helper

The SIP session-helper is a high-performance solution that provides basic support for SIP calls passing through the FortiGate unit by opening SIP and RTP pinholes and by performing NAT of the addresses in SIP messages.

The SIP session helper:

- Understands SIP dialog messages.
- Keeps the states of the SIP transactions between SIP UAs and SIP servers.
- Translates SIP header and SDP information to account for NAT operations performed by the FortiGate unit.
- Opens up and closes dynamic SIP pinholes for SIP signalling traffic.
- Opens up and closes dynamic RTP and RTSP pinholes for RTP and RTSP media traffic.
- Provides basic SIP security as an access control device.
- Uses the intrusion protection (IPS) engine to perform basic SIP protocol checks.

SIP session helper configuration overview

By default FortiOS uses the SIP ALG for SIP traffic. If you want to use the SIP session helper you need to enter the following command:

```
config system settings
   set default-voip-alg-mode kernel-helper-based
end
```

The SIP session helper is set to listen for SIP traffic on TCP or UDP port 5060. SIP sessions using port 5060 accepted by a security policy that does not include a VoIP profile are processed by the SIP session helper.

You can enable and disable the SIP session helper, change the TCP or UDP port that the session helper listens on for SIP traffic, and enable or disable SIP NAT tracing. If the FortiGate unit is operating with multiple VDOMs, each VDOM can have a different SIP session helper configuration.

To have the SIP session helper process SIP sessions you need to add a security policy that accepts SIP sessions on the configured SIP UDP or TCP ports. The security policies can have service set to ANY, or to the SIP pre-defined firewall service, or a custom firewall service. The SIP pre-defined firewall service restricts the security policy to only accepting sessions on UDP port 5060.

If NAT is enabled for security policies that accept SIP traffic, the SIP session helper translates addresses in SIP headers and in the RDP profile and opens up pinholes as required for the SIP traffic. This includes security policies that perform source NAT and security policies that contain virtual IPs that perform destination NAT and port forwarding. No special SIP configuration is required for this address translation to occur, it is all handled automatically by the SIP session helper according to the NAT configuration of the security policy that accepts the SIP session.

To use the SIP session helper you must not add a VoIP profile to the security policy. If you add a VoIP profile, SIP traffic bypasses the SIP session helper and is processed by the SIP ALG.

In most cases you would want to use the SIP ALG since the SIP session helper provides limited functionality. However, the SIP session helper is available and can be useful for high-performance solutions where a high level of SIP security is not a requirement.

Disabling and enabling the SIP session helper

You can use the following steps to disable the SIP session helper. You might want to disable the SIP session helper if you don't want the FortiGate unit to apply NAT or other SIP session help features to SIP traffic. With the SIP session helper disabled, the FortiGate unit can still accept SIP sessions if they are allowed by a security policy, but the FortiGate unit will not be able to open pinholes or NAT the addresses in the SIP messages.

To disable the sip session helper

1. Enter the following command to find the sip session helper entry in the session-helper list:

```
show system session-helper
   .
   .
   .
edit 13
   set name sip
   set port 5060
   set protocol 17
next
   .
   .
   .
```

This command output shows that the sip session helper listens in UDP port 5060 for SIP sessions.

2. Enter the following command to delete session-helper list entry number 13 to disable the sip session helper:

```
config system session-helper
   delete 13
end
```

If you want to use the SIP session helper you can verify whether it is enabled or disabled using the `show system session-helper` command.

You do not have to disable the SIP session helper to use the SIP ALG.

If the SIP session helper has been disabled by being removed from the session-helper list you can use the following command to enable the SIP session helper by adding it back to the session helper list:

```
config system session-helper
   edit 0
      set name sip
      set port 5060
      set protocol 17
end
```

Changing the port numbers that the SIP session helper listens on

You can use the following command to change the port number that the SIP session helper listens on for SIP traffic to 5064. The SIP session helper listens on the same port number for UDP and TCP SIP sessions. In this example, the SIP session helper is session helper 13:

```
config system session-helper
   edit 13
      set port 5064
   end
```

The `config system settings` options `sip-tcp-port`, `sip-udp-port`, and `sip-ssl-port` control the ports that the SIP ALG listens on for SIP sessions. See Changing the port numbers that the SIP ALG listens on on page 2748.

Your FortiGate unit may use a different session helper number for SIP. Enter the following command to view the session helpers:

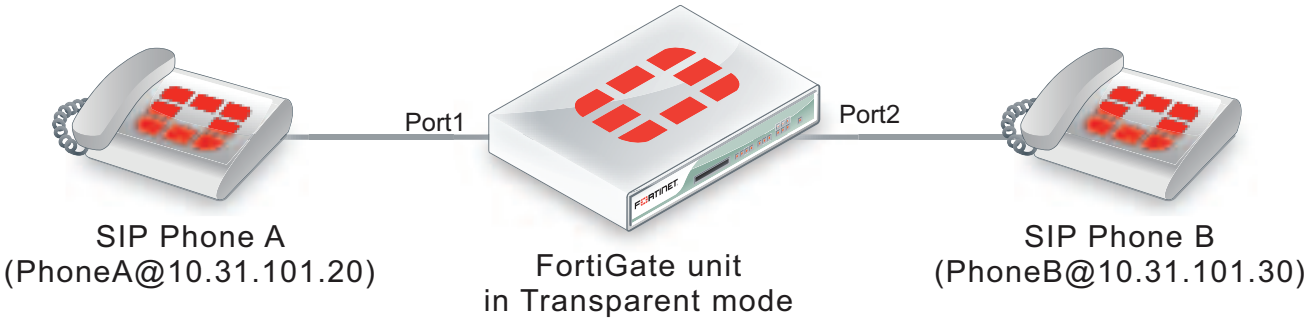
```
show system session-helper
   .
   .
   .
   edit 13
      set name sip
      set port 5060
      set protocol 17
   end
   .
   .
   .
```

Configuration example: SIP session helper in Transparent Mode

The figure below shows an example SIP network consisting of a FortiGate unit operating in Transparent mode between two SIP phones. Since the FortiGate unit is operating in Transparent mode both phones are on the same network and the FortiGate unit and the SIP session helper does not perform NAT. Even though the SIP session helper is not performing NAT you can use this configuration to apply SIP session helper security features to the SIP traffic.

The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A.

SIP network with FortiGate unit in Transparent mode



General configuration steps

The following general configuration steps are required for this SIP configuration that uses the SIP session helper. This example includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the firewall service to ANY to allow traffic other than SIP on UDP port 5060.

This example assumes that you have entered the following command to enable using the SIP session helper:

```
config system settings
   set default-voip-alg-mode kernel-helper-based
end
```

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A.
3. Add a security policy that accepts SIP sessions initiated by Phone B.

Configuration steps - web-based manager

To add firewall addresses for the SIP phones

1. Go to **Policy & Objects > Objects > Addresses**.
2. Select **Create New** to add the following addresses for Phone A and Phone B:

Category	Address

Name	Phone_A
Type	Subnet
Subnet / IP Range	10.31.101.20/255.255.255.255
Interface	port1

Category	Address
Name	Phone_B
Type	Subnet
Subnet / IP Range	10.31.101.30/255.255.255.255
Interface	port2

To add security policies to accept SIP sessions

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New** to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

Incoming Interface	port1
Source Address	Phone_A
Outgoing Interface	port2
Destination Address	Phone_B
Schedule	always
Service	SIP
Action	ACCEPT

4. Select **OK**.
5. Add a security policy to allow Phone B to send SIP request messages to Phone A:

Incoming Interface	port2
Source Address	Phone_B
Outgoing Interface	port1
Destination Address	Phone_A
Schedule	always

Service	SIP
Action	ACCEPT

6. Select **OK**.

Configuration steps - CLI

To add firewall addresses for Phone A and Phone B and security policies to accept SIP sessions

1. Enter the following command to add firewall addresses for Phone A and Phone B.

```
config firewall address
   edit Phone_A
      set associated interface port1
      set type ipmask
      set subnet 10.31.101.20 255.255.255.255
   next
   edit Phone_B
      set associated interface port2
      set type ipmask
      set subnet 10.31.101.30 255.255.255.255
   end
```

2. Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Phone_A
      set dstaddr Phone_B
      set action accept
      set schedule always
      set service SIP
   next
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr Phone_B
      set dstaddr Phone_A
      set action accept
      set schedule always
      set service SIP
      set utm-status enable
   end
```

SIP session helper diagnose commands

You can use the `diagnose sys sip` commands to display diagnostic information for the SIP session helper.

Use the following command to set the debug level for the SIP session helper. Different debug masks display different levels of detail about SIP session helper activity.

```
diagnose sys sip debug-mask <debug_mask_int>
```

Use the following command to display the current list of SIP dialogs being processed by the SIP session help. You can also use the `clear` option to delete all active SIP dialogs being processed by the SIP session helper.

```
diagnose sys sip dialog {clear | list}
```

Use the following command to display the current list of SIP NAT address mapping tables being used by the SIP session helper.

```
diagnose sys sip mapping list
```

Use the following command to display the current SIP session helper activity including information about the SIP dialogs, mappings, and other SIP session help counts. This command can be useful to get an overview of what the SIP session helper is currently doing.

```
diagnose sys sip status
```

The SIP ALG

In most cases you should use the SIP Application Layer Gateway (ALG) for processing SIP sessions. The SIP ALG provides the same basic SIP support as the SIP session helper. Additionally, the SIP ALG provides a wide range of features that protect your network from SIP attacks, can apply rate limiting to SIP sessions, can check the syntax of SIP and SDP content of SIP messages, and provide detailed logging and reporting of SIP activity.

By default all SIP traffic is processed by the SIP ALG. If the policy that accepts the SIP traffic includes a VoIP profile the SIP traffic is processed by that profile. If the policy does not include a SIP profile the SIP traffic is processed by the SIP ALG using the default VoIP profile.

If a FortiGate unit or a VDOM has been configured to use the SIP session helper, you can change this behavior to the default configuration of using the SIP ALG with the following command:

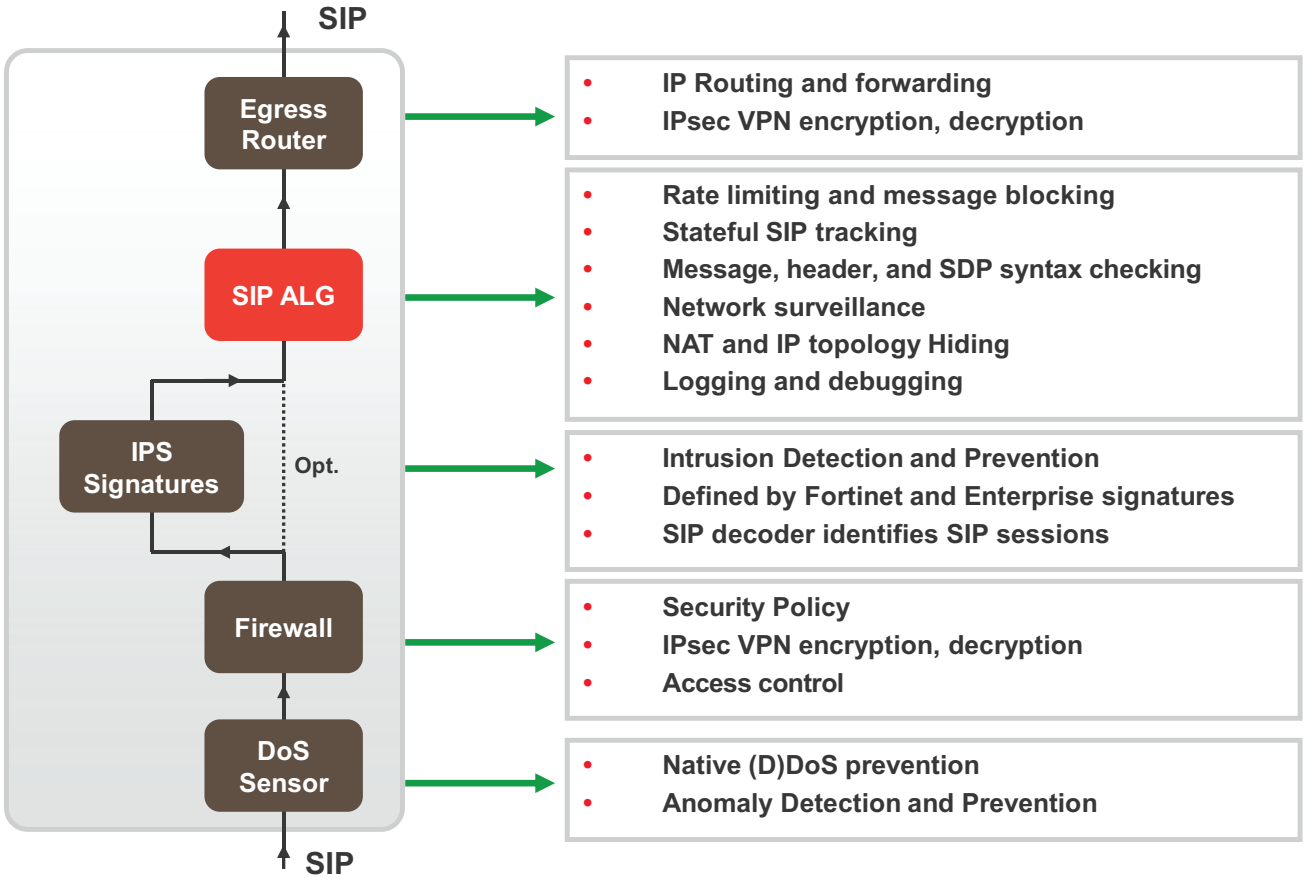
```
config system settings
   set default-voip-alg-mode proxy-based
end
```

As shown in the figure below, the FortiGate SIP ALG intercepts SIP packets after they have been routed by the routing module, accepted by a security policy and passed through DoS and IPS Sensors (if DoS and IPS are enabled). The ALG raises SIP packets to the application layer, analyzes the SIP and SDP addressing information in the SIP messages, makes adjustments (for example, NAT) to this addressing if required, and then sends the packets out the egress interface to their destination.

The SIP ALG provides:

- All the same features as the SIP session helper including NAT and SIP and RTP Pinholes.
- In addition for the ALG you can enable or disable RTP pinholing, SIP register pinholing and SIP contact pinholing. In a signalling only environment where the RTP stream bypasses the FortiGate unit, you can disable RTP pinholing to improve performance.
- SIP TCP and UDP support
- SIP Message order checking
- Configurable Header line length maximums

The SIP ALG works at the application level after ingress packets are accepted by a security policy



- Message fragment assembly (TCP)
- If SIP messages are fragmented across multiple packets, the FortiGate unit assembles the fragments, does inspection and pass the message in its entirety to the SIP server as one packet. This offloads the server from doing all the TCP processing of fragments.
- L4 Protocol Translation
- Message Flood Protection
- Protects a SIP server from intentional or unintentional DoS of flooding INVITE, REGISTER, and other SIP methods by allowing control of the rate that these massages pass through the FortiGate unit.
- SIP message type filtering
- The FortiGate unit can prevent specified SIP message types from passing through the FortiGate unit to a SIP server. For example In a voice only SIP implementation, there may be no need to permit a SUBSCRIBE message to ever make it's way to the SIP call processor. Also, if a SIP server cannot process some SIP message types you can use SIP message type filtering to block them. For example, a SIP server could have a bug that prevents it from processing certain SIP messages. In this case you can temporarily block these message types until problem with the SIP server has been fixed.
- SIP statistics and logging
- SIP over IPv6
- SIP over SSL/TLS

- Deep SIP message syntax checking (also called deep SIP header inspection or SIP fuzzing protection). Prevents attacks that use malformed SIP messages. Can check many SIP headers and SDP statements. Configurable bypass and modification options.
- Hosted NAT traversal, Resolves IP address issue in SIP and SDP lines due to NAT-PT in far end firewall. Important feature for VoIP access networks.
- SIP High Availability (HA), including active-passive clustering and session pickup (session failover) for SIP sessions.
- Geographical Redundancy. In an HA configuration, if the active SIP server fails (missing SIP heartbeat messages or SIP traffic) SIP sessions can be redirected to a secondary SIP server in another location.
- SIP per request method message rate limitation with configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.
- RTP Bypass, Supports configurations with and without RTP pinholing. May inspect and protect SIP signaling only.
- SIP NAT with IP address conservation. Performs SIP and RTP aware IP Network Address translation. Preserves the lost IP address information in the SDP profile i= line for later processing/debugging in the SIP server. See NAT with IP address conservation on page 2778.
- IP topology hiding
- The IP topology of a network can be hidden through NAT and NAPT manipulation of IP and SIP level addressing. For example, see SIP NAT scenario: destination address translation (destination NAT) on page 2766.
- SIP inspection without address translation
- The SIP ALG inspects SIP messages but addresses in the messages are not translated. This feature can be applied to a FortiGate unit operating in Transparent mode or in NAT/Route mode. In Transparent mode you add normal Transparent mode security policies that enable the SIP ALG and include a VoIP profile that causes the SIP ALG to inspect SIP traffic as required. For an example configuration, see Configuration example: SIP in Transparent Mode on page 2754.
- For a FortiGate unit operating in NAT/Route mode, if SIP traffic can pass between different networks without requiring NAT because is supported by the routing configuration, you can add security policies that accept SIP traffic without enabling NAT. In the VoIP profile you can configure the SIP ALG to inspect SIP traffic as required.

SIP ALG configuration overview

To apply the SIP ALG, you add a SIP VoIP profile to a security policy that accepts SIP sessions. All SIP sessions accepted by the security policy will be processed by the SIP ALG using the settings in the VoIP profile. The VoIP profile contains settings that are applied to SIP, Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) and Skinny Call Control Protocol (SCCP) sessions. All SCCP sessions accepted by the security policy are also processed byt the ALG. You configure SIP and SCCP settings separately. SIP settings also apply to SIMPLE sessions.

Enabling VoIP support on the web-based manager

Before you begin to configure VoIP security options, including SIP, from the web-based manager you should go to **System > Config > Features** and turn on VoIP. To find VoIP select the Show More button.

From the CLI you can also enter the following command enable VoIP support on the GUI:

```
config system global
   set gui-voip-profile enable
end
```

VoIP profiles

You can customize the default VoIP profile or add new VoIP profiles.

To add a new VoIP profile from the web-based manager go to **Security Profiles > VoIP** and select **Create New** (the + button).

For SIP, from the web-based manager you can configure the VoIP profile to limit the number of SIP REGISTER and INVITE requests. Many additional options for configuring how the ALG processes SIP sessions are available from the CLI.

For SCCP you can limit the call setup time. Additional SCCP options are available from the CLI.

Use the following command to add a VoIP profile named VoIP_Pro_1 from the CLI:

```
config voip profile
   edit VoIP_Pro_1
end
```

FortiGate units include two pre-defined VoIP profiles. On the web-based manager these profiles look identical. However, the CLI-only settings result in the following functionality.

default	The most commonly used VoIP profile. This profile enables both SIP and SCCP and places the minimum restrictions on what calls will be allowed to negotiate. This profile allows normal SCCP, SIP and RTP sessions and enables the following security settings: • `block-long-lines` to block SIP messages with lines that exceed maximum line lengths. • `block-unknown` to block unrecognized SIP request messages. • `open-record-route-pinhole` to open pinholes for Record-Route messages. • `log-violations` to write log messages that record SIP violations. • `log-call-summary` to write log messages that record SIP call progress (similar to DLP archiving). • `nat-trace` (see NAT with IP address conservation on page 2778). • `contact-fixup` perform NAT on the IP addresses and port numbers in SIP headers in SIP CONTACT messages even if they don't match the session's IP address and port numbers. • `ips-rtp` to enable IPS in security policies that also accept SIP sessions to protect the SIP traffic from SIP-based attacks.
strict	This profile is available for users who want to validate SIP messages and to only allow SIP sessions that are compliant with RFC 3261. In addition to the settings in the default VoIP profile, the strict profile sets all SIP deep message inspection header checking options to `discard`. So the strict profile blocks and drops SIP messages that contain malformed SIP or SDP lines that can be detected by the ALG. For more information about SIP deep header inspection, see Deep SIP message inspection on page 2792.

Neither of the default profiles applies SIP rate limiting. To apply more ALG features to SIP sessions you can clone (copy) the pre-defined VoIP profiles and make your own modifications to them. For example, to clone the default profile and configure the limit for SIP NOTIFY request messages to 1000 messages per second per security policy and block SIP INFO request messages.

```
config voip profile
   clone default to my_voip_pro
   edit my_voip_pro
      config sip
         set notify-rate 1000
         set block-info enable
      end
   end
```

Changing the port numbers that the SIP ALG listens on

Most SIP configurations use TCP or UDP port 5060 for SIP sessions and port 5061 for SIP SSL sessions. If your SIP network uses different ports for SIP sessions you can use the following command to configure the SIP ALG to listen on a different TCP, UDP, or SSL ports. For example, to change the TCP port to 5064, the UDP port to 5065, and the SSL port to 5066.

```
config system settings
   set sip-tcp-port 5064
   set sip-udp-port 5065
   set sip-ssl-port 5066
end
```

You also configure the SIP ALG to listen in two different TCP ports and two different UDP ports for SIP sessions. For example, if you receive SIP TCP traffic on port 5060 and 5064 and UDP traffic on ports 5061 and 5065 you can enter the following command to receive the SIP traffic on all of these ports:

```
config system settings
   set sip-tcp-port 5060 5064
   set sip-udp-port 5061 5065
end
```

Disabling the SIP ALG in a VoIP profile

SIP is enabled by default in a VoIP profile. If you are just using the VoIP profile for SCCP you can use the following command to disable SIP in the VoIP profile.

```
config voip profile
edit VoIP_Pro_2
  config sip
    set status disable
  end
   end
```

SIP ALG get and diagnose commands

You can use the following commands to display diagnostic information for the SIP ALG.

Use the following command to list all active SIP calls being processed by the SIP ALG. You can also use the `clear` option to delete all active SIP calls being processed by the SIP ALG.

```
diagnose sys sip-proxy calls {clear | list}
```

Use the following commands to use filters to display specific information about the SIP ALG and the session that it is processing.

```
diagnose sys sip-proxy filter <filter_options>
diagnose sys sip-proxy log-filter <filter_options>
```

Use the following command to display the active SIP rate limiting meters and their current settings.

```
diagnose sys sip-proxy meters list
```

Use the following command to display status information about the SIP sessions being processed by the SIP ALG. You can also clear all SIP ALG statistics.

```
diagnose sys sip-proxy stats {clear | list}
```

Conflicts between the SIP ALG and the session helper

If you suspect that the SIP session helper is being used instead of the ALG, you can use the `diagnose sys sip` command to determine if the SIP session helper is processing SIP sessions. For example, the following command displays the overall status of the SIP sessions being processed by the SIP session helper:

The `diagnose sys sip` commands only display current status information. To see activity the SIP session helper has to actually be processing SIP sessions when you enter the command. For example, if the SIP session helper had been used for processing calls that ended 5 minutes ago, the command output would show no SIP session helper activity.

```
diagnose sys sip status
dialogs: max=32768, used=0
mappings: used=0
dialog hash by ID: size=2048, used=0, depth=0
dialog hash by RTP: size=2048, used=0, depth=0
mapping hash: size=2048, used=0, depth=0
count0: 0
count1: 0
count2: 0
count3: 0
count4: 0
```

This command output shows that the session helper is not processing SIP sessions because all of the used and count fields are 0. If any of these fields contains non-zero values then the SIP session helper may be processing SIP sessions.

Also, you can check to see if some ALG-only features are not being applied to all SIP sessions. For example, FortiView pages displays statistics for SIP and SCCP calls processed by the ALG but not for calls processed by the session helper. So if you see fewer calls than expected the session helper may be processing some of them.

Finally, you can check the policy usage and session information dashboard widgets to see if SIP sessions are being accepted by the wrong security policies.

Stateful SIP tracking, call termination, and session inactivity timeout

The SIP ALG tracks SIP dialogs over their lifespan between the first INVITE message and the Final 200 OK and ACK messages. For every SIP dialog, stateful SIP tracking reviews every SIP message and makes adjustment to SIP tracking tables as required. These adjustments include source and destination IP addresses, address translation, dialog expiration information, and media stream port changes. Such changes can also result in dynamically opening and closing pinholes. You can use the `diagnose sys sip-proxy stats list` and the `diagnose sys sip-proxy filter` command to view the SIP call data being tracked by the SIP ALG.

The SIP ALG uses the SIP Expires header line to time out a SIP dialog if the dialog is idle and a Re-INVITE or UPDATE message is not received. The SIP ALG gets the Session-Expires value, if present, from the 200 OK response to the INVITE message. If the SIP ALG receives an INVITE before the session times out, all timeout values are reset to the settings in the new INVITE message or to default values. As a precautionary measure, the

SIP ALG uses hard timeout values to set the maximum amount of time a call can exist. This ensures that the FortiGate unit is protected if a call ends prematurely.

When a SIP dialog ends normally, the SIP ALG deletes the SIP call information and closes open pinholes. A SIP call can also end abnormally due to an unexpected signaling or transport event that cuts off the call. When a call ends abnormally the SIP messages to end the call may not be sent or received. A call can end abnormally for the following reasons:

- Phones or servers crash during a call and a BYE message is not received.
- To attack a SIP system, a malicious user never send a BYE message.
- Poor implementations of SIP fail to process Record-Route messages and never send a BYE message.
- Network failures prevent a BYE message from being received.

Any phone or server in a SIP call can cancel the call by sending a CANCEL message. When a CANCEL message is received by the FortiGate unit, the SIP ALG closes open pinholes. Before terminating the call, the ALG waits for the final 200 OK message.

The SIP ALG can be configured to terminate SIP calls if the SIP dialog message flow or the call RTP (media) stream is interrupted and does not recover. You can use the following commands to configure terminating inactive SIP sessions and to set timers or counters to control when the call is terminated by the SIP ALG.

Adding a media stream timeout for SIP calls

Use the following command in a VoIP profile to terminate SIP calls accepted by a security policy containing the VoIP profile when the RTP media stream is idle for 100 seconds.

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set call-keepalive 100
      end
   end
```

You can adjust this setting between 1 and 10,080 seconds. The default call keepalive setting of 0 disables terminating a call if the media stream is interrupted. Set call keepalive higher if your network has latency problems that could temporarily interrupt media streams. If you have configured call keepalive and the FortiGate unit terminates calls unexpectedly you can increase the call keepalive time to resolve the problem.

Call keep alive should be used with caution because enabling this feature results in extra FortiGate CPU overhead and can cause delay/jitter for the VoIP call. Also, the FortiGate unit terminates the call without sending SIP messages to end the call. And if the SIP endpoints send SIP messages to terminate the call they will be blocked by the FortiGate unit if they are sent after the FortiGate unit terminates the call.

Adding an idle dialog setting for SIP calls

Use the following command in a VoIP profile to terminate SIP calls when for a single security policy, when the configured number of SIP calls (or dialogs) has stopped receiving SIP messages or has not received legitimate SIP messages. Using this command you can configure how many dialogs that have been accepted by a security policy that the VoIP profile is added to become idle before the SIP ALG deletes the oldest ones. The following command sets the maximum number of idle dialogs to 200:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set max-idle-dialogs 200
```

```
        end
    end
```

Idle dialogs would usually be dialogs that have been interrupted because of errors or problems or as the result of a SIP attack that opens a large number of SIP dialogs without closing them. This command provides a way to remove these dialogs from the dialog table and recover memory and resources being used by these open and idle dialogs.

You can adjust this setting between 1 and a very high number. The default maximum idle dialogs setting of 0 disables this feature. Set maximum dialogs higher if your network has latency problems that could temporarily interrupt SIP messaging. If you have configured max idle dialogs and the FortiGate unit terminates calls unexpectedly you can increase the max idle dialogs number to resolve the problem.

Changing how long to wait for call setup to complete

In some cases and some configurations your SIP system may experience delays during call setup. If this happens, some SIP ALG timers may expire before call setup is complete and drop the call. In some cases you may also want to reduce the amount of time the SIP ALG allows for call setup to complete.

You can use the `provisional-invite-expiry-time` SIP VoIP profile option to control how long the SIP ALG waits for provisional INVITE messages before assuming that the call setup has been interrupted and the SIP call should be dropped. The default value for this timer is 210 seconds. You can change it to between 10 and 3600 seconds.

Use the following command to change the expiry time to 100 seconds.

```
config voip profile
   edit Profile_name
      config sip
         set provisional-invite-expiry-time 100
      end
end
```

SIP and RTP/RTCP

FortiGate units support the Real Time Protocol (RTP) application layer protocol for the VoIP call audio stream. RTP uses dynamically assigned port numbers that can change during a call. SIP control messages that start a call and that are sent during the call inform callers of the port number to use and of port number changes during the call.

During a call, each RTP session will usually have a corresponding Real Time Control Protocol (RTCP) session. By default, the RTCP session port number is one higher than the RTP port number.

The RTP port number is included in the `m=` part of the SDP profile. In the example above, the SIP INVITE message includes RTP port number is 49170 so the RTCP port number would be 49171. In the SIP response message the RTP port number is 3456 so the RTCP port number would be 3457.

How the SIP ALG creates RTP pinholes

The SIP ALG requires the following information to create a pinhole. The SIP ALG finds this information in SIP messages and some is provided by the SIP ALG:

Protocol	UDP (Extracted from SIP messages by the SIP ALG.)
Source IP	Any
Source port	Any
Destination IP	The SIP ALG extracts the destination IP address from the c= line in the SDP profile. The c= line can appear in either the session or media part of the SDP profile. The SIP ALG uses the IP address in the c= line of the media part of the SDP profile first. If the media part does not contain a c= line, the SIP ALG checks the c= line in the session part of the SDP profile. If the session part of the profile doesn't contain a c= line the packet is dropped. Pinholes for RTP and RTCP sessions share the same destination IP address.
Destination port	The SIP ALG extracts the destination port number for RTP from the m= field and adds 1 to this number to get the RTCP port number.
Lifetime	The length of time during which the pinhole will be open. When the lifetime ends, the SIP ALG removes the pinhole.

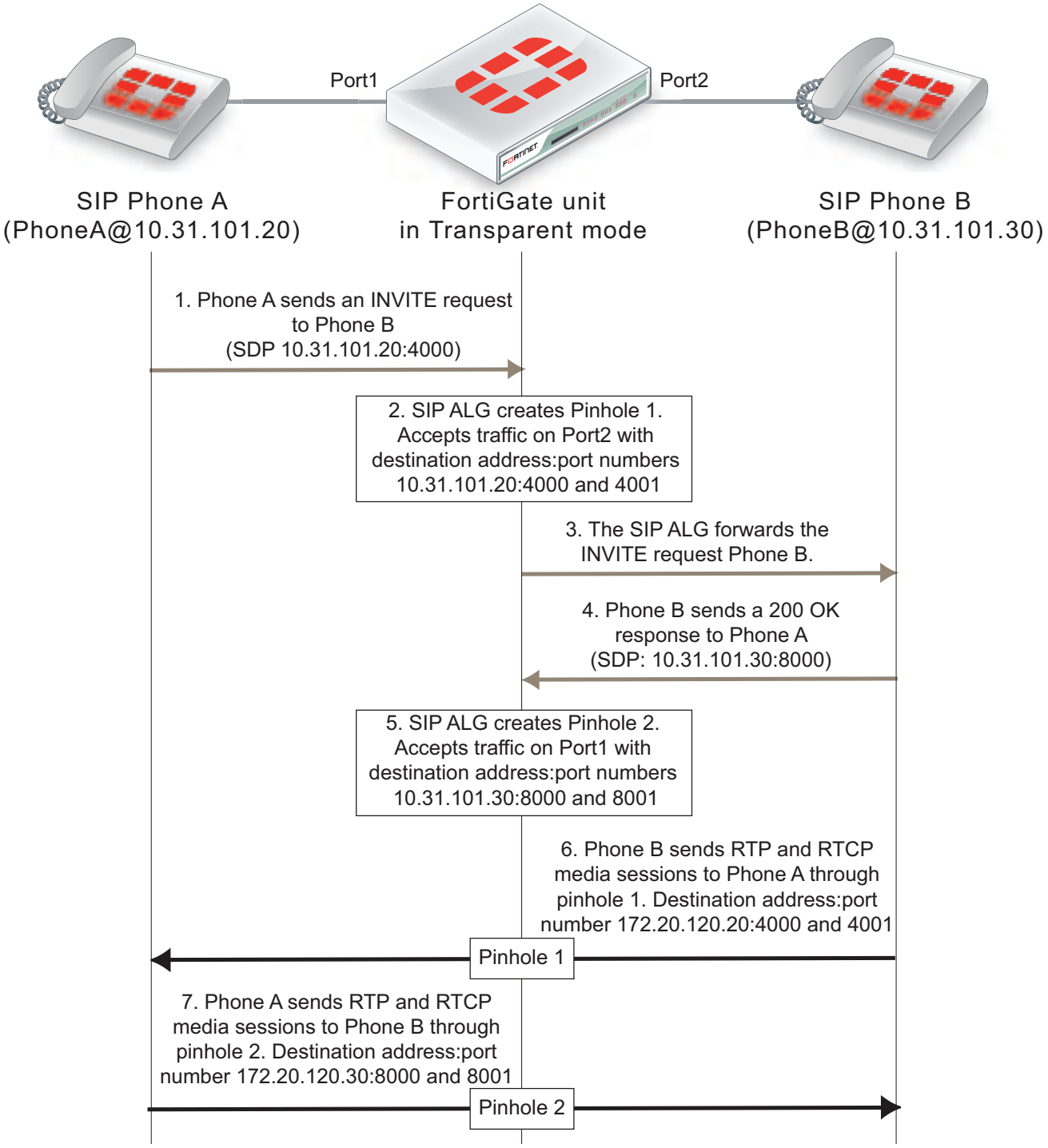
The SIP ALG keeps RTP pinholes open as long as the SIP session is alive. When the associated SIP session is terminated by the SIP ALG or the SIP phones or servers participating in the call, the RTP pinhole is closed.

The figure below shows a simplified call setup sequence that shows how the SIP ALG opens pinholes. Phone A and Phone B are installed on either side of a FortiGate unit operating in Transparent mode. Phone A and Phone B are on the same subnet. The FortiGate unit includes a security policy that accepts SIP sessions from port1 to port2 and from port2 to port1. The FortiGate unit does not require an RTP security policy, just the SIP policy.

You can see from this diagram that the SDP profile in the INVITE request from Phone A indicates that Phone A is expecting to receive a media stream sent to its IP address using port 4000 for RTP and port 4001 for RTCP. The SIP ALG creates pinhole 1 to allow this media traffic to pass through the FortiGate unit. Pinhole 1 is opened on the Port2 interface and will accept media traffic sent from Phone B to Phone A.

When Phone B receives the INVITE request from Phone A, Phone B will know to send media streams to Phone A using destination IP address 10.31.101.20 and ports 4000 and 4001. The 200 OK response sent from Phone B indicates that Phone B is expecting to receive a media stream sent to its IP address using ports 8000 and 8001. The SIP ALG creates pinhole 2 to allow this media traffic to pass through the FortiGate unit. Pinhole 2 is opened on the Port1 interface and will accept media traffic sent from Phone A to Phone B.

SIP call setup with a FortiGate unit in Transparent mode

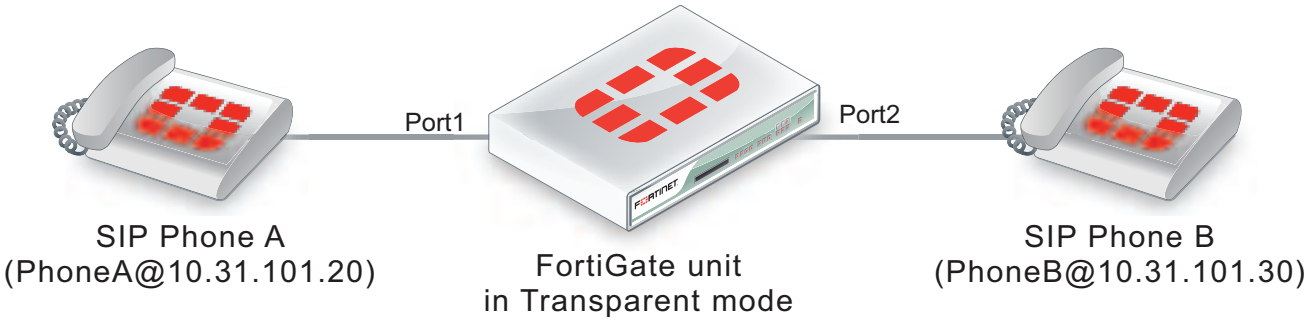


Configuration example: SIP in Transparent Mode

The figure below hows an example SIP network consisting of a FortiGate unit operating in Transparent mode between two SIP phones. Since the FortiGate unit is operating in Transparent mode both phones are on the same network and the FortiGate unit and the SIP ALG does not perform NAT. Even though the SIP ALG is not performing NAT you can use this configuration to apply SIP security features to the SIP traffic.

The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A.

SIP network with FortiGate unit in Transparent mode



General configuration steps

The following general configuration steps are required for this SIP configuration. This example uses the default VoIP profile. The example also includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the security service to ANY to allow traffic other than SIP on UDP port 5060.

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A and includes the default VoIP profile.
3. Add a security policy that accepts SIP sessions initiated by Phone B and includes the default VoIP profile.

Configuration steps - web-based manage

Before you begin this procedure you may have to go to **System > Config > Features** and turn on VoIP. To find VoIP select the Show More button.

To add firewall addresses for the SIP phones

1. Go to **Policy & Objects > Objects > Addresses**.
2. Add the following addresses for Phone A and Phone B:

Category	Address

Name	Phone_A
Type	Subnet
Subnet / IP Range	10.31.101.20/255.255.255.255
Interface	port1

Category	Address
Name	Phone_B
Type	Subnet
Subnet / IP Range	10.31.101.30/255.255.255.255
Interface	port2

To add security policies to apply the SIP ALG to SIP sessions

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New** to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

Incoming Interface	port1
Source Address	Phone_A
Outgoing Interface	port2
Destination Address	Phone_B
Schedule	always
Service	SIP
Action	ACCEPT

4. Turn on **VoIP** and select the **default** VoIP profile.
5. Select **OK**.
6. Add a security policy to allow Phone B to send SIP request messages to Phone A:

Incoming Interface	port2
Source Address	Phone_B
Outgoing Interface	port1
Destination Address	Phone_A

Schedule	always
Service	SIP
Action	ACCEPT

7. Turn on **VoIP** and select the **default** VoIP profile.
8. Select **OK**.

Configuration steps - CLI

To add firewall addresses for Phone A and Phone B and security policies to apply the SIP ALG to SIP sessions

1. Enter the following command to add firewall addresses for Phone A and Phone B.

```
config firewall address
   edit Phone_A
      set associated interface port1
      set type ipmask
      set subnet 10.31.101.20 255.255.255.255
   next
   edit Phone_B
      set associated interface port2
      set type ipmask
      set subnet 10.31.101.30 255.255.255.255
   end
```

2. Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Phone_A
      set dstaddr Phone_B
      set action accept
      set schedule always
      set service SIP
      set utm-status enable
      set voip-profile default
   next
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr Phone_B
      set dstaddr Phone_A
      set action accept
      set schedule always
      set service SIP
      set utm-status enable
      set voip-profile default
   end
```

RTP enable/disable (RTP bypass)

You can configure the SIP ALG to stop from opening RTP pinholes. Called RTP bypass, this configuration can be used when you want to apply SIP ALG features to SIP signalling messages but do not want the RTP media streams to pass through the FortiGate unit. The FortiGate unit only acts as a signalling firewall and RTP media session bypass the FortiGate unit and no pinholes need to be created.

Enter the following command to enable RTP bypass in a VoIP profile by disabling opening RTP pinholes:

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set rtp disable
      end
end
```

Opening and closing SIP register, contact, via and record-route pinholes

You can use the `open-register-pinhole`, `open-contact-pinhole`, `open-via-port`, and `open-record-route-pinhole` VoIP profile CLI options to control whether the FortiGate unit opens various pinholes.

If `open-register-pinhole` is enabled (the default setting) the FortiGate unit opens pinholes for SIP Register request messages. You can disable `open-register-pinhole` so that the FortiGate unit does not open pinholes for SIP Register request messages.

If `open-contact-pinhole` is enabled (the default setting) the FortiGate unit opens pinholes for non-Register SIP request messages. You can disable `open-contact-pinhole` so that the FortiGate unit does not open pinholes for non-register requests. Non-register pinholes are usually opened for SIP INVITE requests.

If `open-via-pinhole` is disabled (the default setting) the FortiGate unit does not open pinholes for Via messages. You can enable `open-via-pinhole` so that the FortiGate unit opens pinholes for Via messages.

If `open-record-route-pinhole` is enabled (the default setting) the FortiGate unit opens pinholes for Record-Route messages. You can disable `open-record-route-pinhole` so that the FortiGate unit does not open pinholes for Record-Route messages.

Usually you would want to open these pinholes. Keeping them closed may prevent SIP from functioning properly through the FortiGate unit. They can be disabled, however, for interconnect scenarios (where all SIP traffic is between proxies and traveling over a single session). In some cases these settings can also be disabled in access scenarios if it is known that all users will be registering regularly so that their contact information can be learned from the register request.

You might want to prevent pinholes from being opened to avoid creating a pinhole for every register or non-register request. Each pinhole uses additional system memory, which can affect system performance if there are hundreds or thousands of users, and requires refreshing which can take a relatively long amount of time if there are thousands of active calls.

To configure a VoIP profile to prevent opening register and non-register pinholes:

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set open-register-pinhole disable
         set open-contact-pinhole disable
```

```
        end
    end
```

In some cases you may not want to open pinholes for the port numbers specified in SIP Contact headers. For example, in an interconnect scenario when a FortiGate unit is installed between two SIP servers and the only SIP traffic through the FortiGate unit is between these SIP servers pinholes may not need to be opened for the port numbers specified in the Contact header lines.

If you disable `open-register-pinhole` then pinholes are not opened for ports in Contact header lines in SIP Register messages. If you disable `open-contact-pinhole` then pinholes are not opened for ports in Contact header lines in all SIP messages except SIP Register messages.

Accepting SIP register responses

You can enable the VoIP profile `open-via-pinhole` options to accept a SIP Register response message from a SIP server even if the source port of the Register response message is different from the destination port.

Most SIP servers use 5060 as the source port in the SIP register response. Some SIP servers, however, may use a different source port. If your SIP server uses a different source port, you can enable `open-via-pinhole` and the SIP ALG will create a temporary pinhole when the Register request from a SIP client includes a different source port. The FortiGate unit will accept a SIP Register response with any source port number from the SIP server.

Enter the following command to enable accepting any source port from a SIP server:

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set open-via-pinhole enable
      end
end
```

How the SIP ALG performs NAT

In most Network Address Translation (NAT) configurations, multiple hosts in a private network share a single public IP address to access the Internet. For sessions originating on the private network for the Internet, NAT replaces the private IP address of the PC in the private subnet with the public IP address of the NAT device. The NAT device converts the public IP address for responses from the Internet back into the private address before sending the response over the private network to the originator of the session.

Using NAT with SIP is more complex because of the IP addresses and media stream port numbers used in SIP message headers and bodies. When a caller on the private network sends a SIP message to a phone or SIP server on the Internet, the SIP ALG must translate the private network addresses in the SIP message to IP addresses and port numbers that are valid on the Internet. When the response message is sent back to the caller, the SIP ALG must translate these addresses back to valid private network addresses.

In addition, the media streams generated by the SIP session are independent of the SIP message sessions and use varying port numbers that can also change during the media session. The SIP ALG opens pinholes to accept these media sessions, using the information in the SIP messages to determine the pinholes to open. The ALG may also perform port translation on the media sessions.

When an INVITE message is received by the SIP ALG, the FortiGate unit extracts addressing and port number information from the message header and stores it in a SIP dialog table. Similar to an IP session table the data in the dialog table is used to translate addresses in subsequent SIP messages that are part of the same SIP call.

When the SIP ALG receives a response to the INVITE message arrives, (for example, an ACK or 200 OK), the SIP ALG compares the addresses in the message fields against the entries in the SIP dialog table to identify the call context of the message. The SIP ALG then translates addresses in the SIP message before forwarding them to their destination.

The addressing and port number information in SDP fields is used by the ALG to reserve ports for the media session and create a NAT mapping between them and the ports in the SDP fields. Because SDP uses sequential ports for the RTP and RTCP channels, the ALG provides consecutive even-odd ports.

Source address translation

When a SIP call is started by a phone on a private network destined for a phone on the Internet, only source address translation is required. The phone on the private network attempts to contact the actual IP address of the phone on the Internet. However, the source address of the phone on the private network is not routable on the Internet so the SIP ALG must translate all private IP addresses in the SIP message into public IP addresses.

To configure the FortiGate for source address translation you add security policy that accepts sessions from the internal network destined for the Internet. You must enable NAT for the security policy and add a VoIP profile.

When a SIP request is received from the internal to the external network, the SIP ALG replaces the private network IP addresses and port numbers in the SIP message with the IP address of the FortiGate interface connected to the Internet. Depending on the content of the message, the ALG translates addresses in the Via:, Contact:, Route:, and Record-Route: SIP header fields. The message is then forwarded to the destination (either a VoIP phone or a SIP server on the Internet).

The VoIP phone or server in the Internet sends responses to these SIP messages to the external interface of the FortiGate unit. The addresses in the response messages are translated back into private network addresses and the response is forwarded to the originator of the request.

For the RTP communication between the SIP phones, the SIP ALG opens pinholes to allow media through the FortiGate unit on the dynamically assigned ports negotiated based on information in the SDP and the Via:, Contact:, and Record-Route: header fields. The pinholes also allow incoming packets to reach the Contact:, Via:, and Record-Route: IP addresses and ports. When processing return traffic, the SIP ALG inserts the original Contact:, Via:, Route:, and Record-Route: SIP fields back into the packets.

Destination address translation

Incoming calls are directed from a SIP phone on the Internet to the interface of the FortiGate unit connected to the Internet. To receive these calls you must add a security policy to accept SIP sessions from the Internet. The security policy requires a firewall virtual IP. SIP INVITE messages from the Internet connect to the external IP address of the virtual IP. The SIP ALG uses the destination address translation defined in the virtual IP to translated the addresses in the SIP message to addresses on the private network.

When a 200 OK response message arrives from the private network, the SIP ALG translates the addresses in the message to Internet addresses and opens pinholes for media sessions from the private network to the Internet.

When the ACK message is received for the 200 OK, it is also intercepted by the SIP ALG. If the ACK message contains SDP information, the SIP ALG checks to determine if the IP addresses and port numbers are not changed from the previous INVITE. If they are, the SIP ALG deletes pinholes and creates new ones as required. The ALG also monitors the Via:, Contact:, and Record-Route: SIP fields and opens new pinholes as required.

Call Re-invite messages

SIP Re-INVITE messages can dynamically add and remove media sessions during a call. When new media sessions are added to a call the SIP ALG opens new pinholes and update SIP dialog data. When media sessions are ended, the SIP ALG closes pinholes that are no longer needed and removes SIP dialog data.

How the SIP ALG translates IP addresses in SIP headers

The SIP ALG applies NAT to SIP sessions by translating the IP addresses contained in SIP headers. For example, the following SIP message contains most of the SIP fields that contain addresses that need to be translated:

```
INVITE PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 172.20.120.50:5434
From: PhoneA@10.31.101.20
To: PhoneB@172.20.120.30
Call-ID: a12abcde@172.20.120.50
Contact: PhoneA@10.31.101.20:5434
Route: <sip:example@172.20.120.50:5060>
Record-Route: <sip:example@172.20.120.50:5060>
```

How IP address translation is performed depends on whether source NAT or destination NAT is applied to the session containing the message:

Source NAT translation of IP addresses in SIP messages

Source NAT translation occurs for SIP messages sent from a phone or server on a private network to a phone or server on the Internet. The source addresses in the SIP header fields of the message are typically set to IP addresses on the private network. The SIP ALG translates these addresses to the address the FortiGate unit interface connected to the Internet.

Source NAT translation of IP addresses in SIP request messages

SIP header	NAT action
To:	None
From:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.
Call-ID:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.
Via:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.
Request-URI:	None
Contact:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.
Record-Route:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.
Route:	Replace private network address with IP address of FortiGate unit interface connected to the Internet.

Response messages from phones or servers on the Internet are sent to the FortiGate unit interface connected to the Internet where the destination addresses are translated back to addresses on the private network before forwarding the SIP response message to the private network.

Source NAT translation of IP addresses in SIP response messages

SIP header	NAT action
To:	None
From:	Replace IP address of FortiGate unit interface connected to the Internet with private network address.
Call-ID:	Replace IP address of FortiGate unit interface connected to the Internet with private network address.
Via:	Replace IP address of FortiGate unit interface connected to the Internet with private network address.
Request-URI:	N/A
Contact:	None
Record-Route:	Replace IP address of FortiGate unit interface connected to the Internet with private network address.
Route:	Replace IP address of FortiGate unit interface connected to the Internet with private network address.

Destination NAT translation of IP addresses in SIP messages

Destination NAT translation occurs for SIP messages sent from a phone or server on the Internet to a firewall virtual IP address. The destination addresses in the SIP header fields of the message are typically set to the virtual IP address. The SIP ALG translates these addresses to the address of a SIP server or phone on the private network on the other side of the FortiGate unit.

Destination NAT translation of IP addresses in SIP request messages

SIP header	NAT action
To:	Replace VIP address with address on the private network as defined in the firewall virtual IP.
From:	None
Call-ID:	None
Via:	None
Request-URI:	Replace VIP address with address on the private network as defined in the firewall virtual IP.
Contact:	None
Record-Route:	None
Route:	None

SIP response messages sent in response to the destination NAT translated messages are sent from a server or a phone on the private network back to the originator of the request messages on the Internet. These reply messages are accepted by the same security policy that accepted the initial request messages, The firewall VIP in the original security policy contains the information that the SIP ALG uses to translate the private network source addresses in the SIP headers into the firewall virtual IP address.

Destination NAT translation of IP addresses in SIP response messages

SIP header	NAT action
To:	None
From:	Replace private network address with firewall VIP address.
Call-ID:	None
Via:	None
Request-URI:	N/A
Contact:	Replace private network address with firewall VIP address.
Record-Route:	Replace private network address with firewall VIP address.
Route:	None

How the SIP ALG translates IP addresses in the SIP body

The SDP session profile attributes in the SIP body include IP addresses and port numbers that the SIP ALG uses to create pinholes for the media stream.

The SIP ALG translates IP addresses and port numbers in the o=, c=, and m= SDP lines. For example, in the following lines the ALG could translate the IP addresses in the o= and c= lines and the port number (49170) in the m= line.

```
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
```

If the SDP session profile includes multiple RTP media streams, the SIP ALG opens pinholes and performs the required address translation for each one.

The two most important SDP attributes for the SIP ALG are c= and m=. The c= attribute is the connection information attribute. This field can appear at the session or media level. The syntax of the connection attribute is:

```
c=IN {IPV4 | IPV6} <destination_ip_address>
```

Where

- `IN` is the network type. FortiGate units support the `IN` or Internet network type.
- `{IPV4 | IPV6}` is the address type. FortiGate units support IPv4 or IPv6 addresses in SDP statements. However, FortiGate units do not support all types of IPv6 address translation. See "SIP over IPv6".
- `<destination_IP_address>` is the unicast numeric destination IP address or domain name of the connection in either IPv4 or IPv6 format.

The syntax of the media attribute is:

```
m=audio <port_number> RTP <format_list>
```

Where

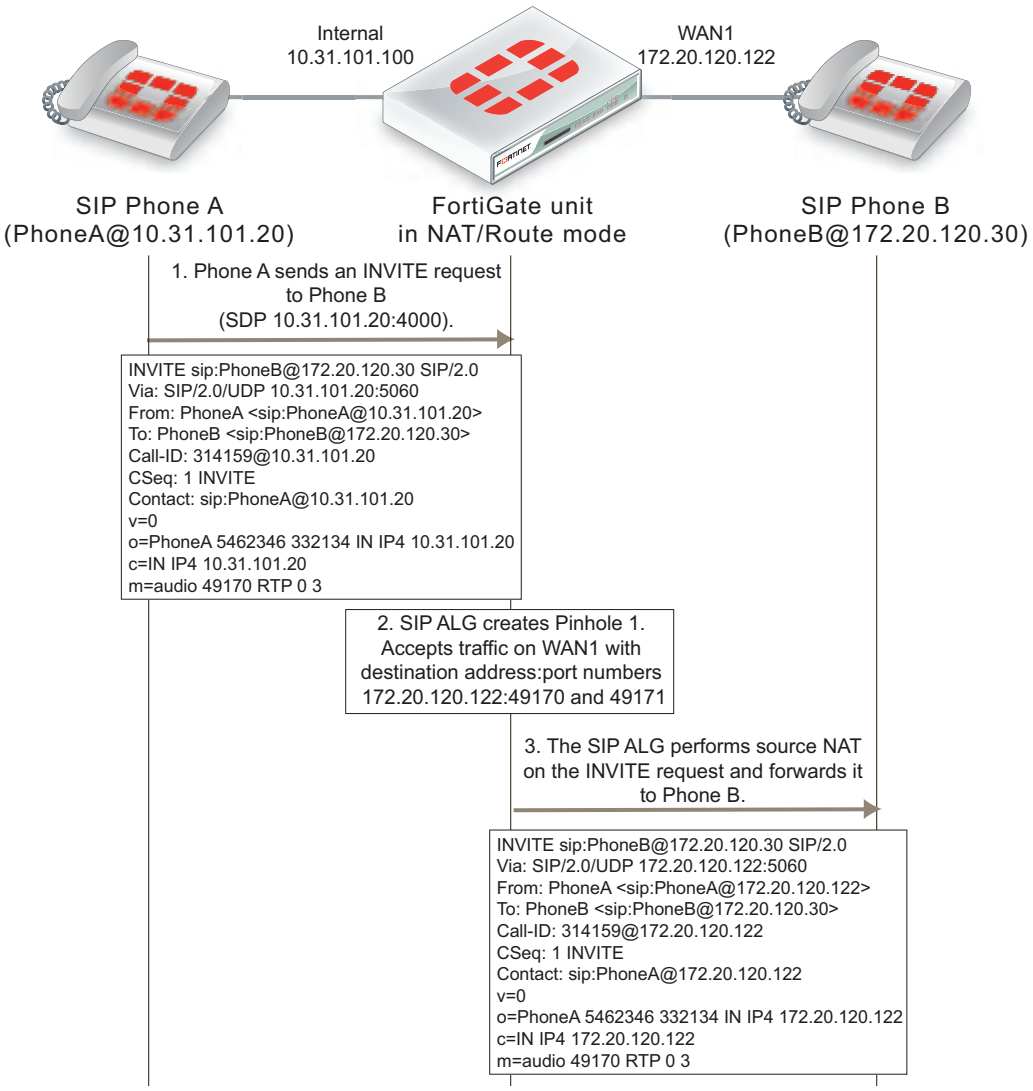
- `audio` is the media type. FortiGate units support the `audio` media type.
- `<port_number>` is the destination port number used by the media stream.
- `RTP` is the application layer transport protocol used for the media stream. FortiGate units support the Real Time Protocol (RTP) transport protocol.
- `<format_list>` is the format list that provides information about the application layer protocol that the media uses.

SIP NAT scenario: source address translation (source NAT)

The following figures show a source address translation scenario involving two SIP phones on different networks, separated by a FortiGate unit. In the scenario, SIP Phone A sends an INVITE request to SIP Phone B and SIP Phone B replies with a 200 OK response and then the two phones start media streams with each other.

To simplify the diagrams, some SIP messages are not included (for example, the Ringing and ACK response messages) and some SIP header lines and SDP profile lines have been removed from the SIP messages.

SIP source NAT scenario part 1: INVITE request sent from Phone A to Phone B



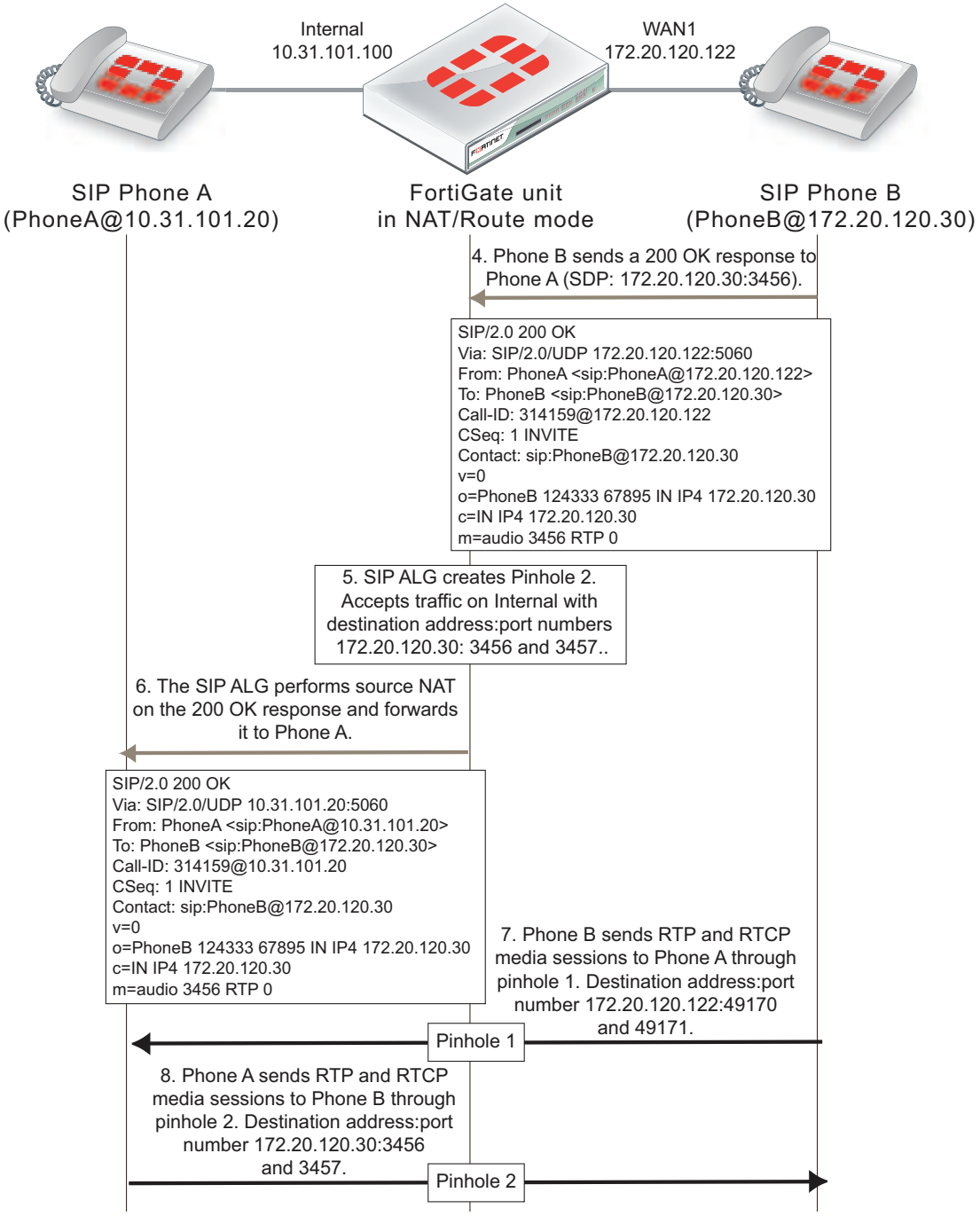
For the replies to SIP packets sent by Phone A to be routable on Phone Bs network, the FortiGate unit uses source NAT to change their source address to the address of the WAN1 interface. The SIP ALG makes similar changes the source addresses in the SIP headers and SDP profile. For example, the original INVITE request from Phone A includes the address of Phone A (10.31.101.20) in the from header line. After the INVITE request passes through the FortiGate unit, the address of Phone A in the From SIP header line is translated to 172.20.120.122, the address of the FortiGate unit WAN1 interface. As a result, Phone B will reply to SIP messages from Phone A using the WAN1 interface IP address.

The FortiGate unit also opens a pinhole so that it can accept media sessions sent to the WAN1 IP address using the port number in the m= line of the INVITE request and forward them to Phone A after translating the destination address to the IP address of Phone A.

Phone B sends the 200 OK response to the INVITE message to the WAN1 interface. The SDP profile includes the port number that Phone B wants to use for its media stream. The FortiGate unit forwards 200 OK response to Phone A after translating the addresses in the SIP and SDP lines back to the IP address of Phone A. The SIP ALG

also opens a pinhole on the Internal interface that accepts media stream sessions from Phone A with destination address set to the IP address of Phone B and using the port that Phone B added to the SDP m= line.

SIP source NAT scenario part 2: 200 OK returned and media streams established

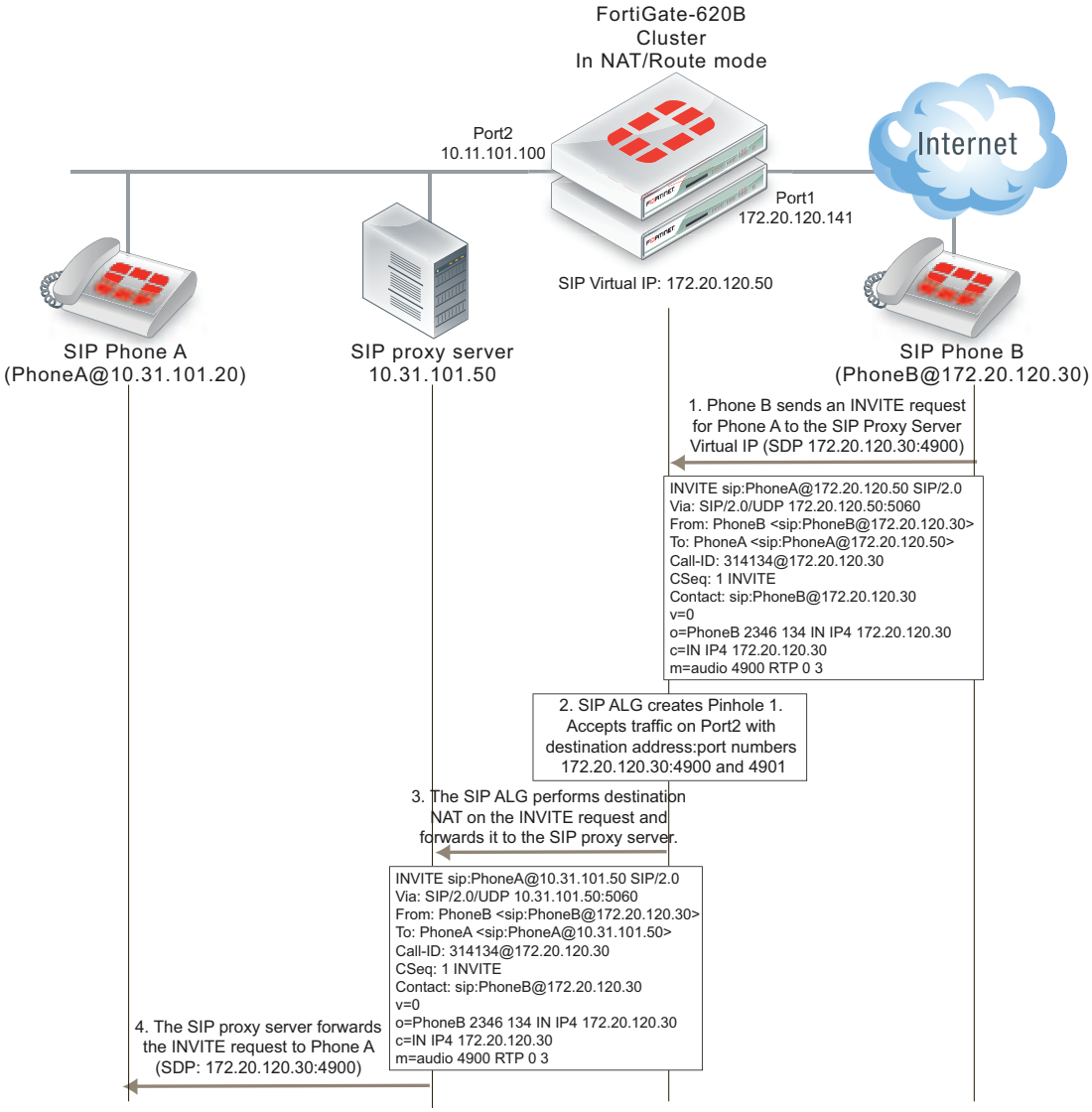


SIP NAT scenario: destination address translation (destination NAT)

The following figures show how the SIP ALG translates addresses in a SIP INVITE message sent from SIP Phone B on the Internet to SIP Phone A on a private network using the SIP proxy server. Because the addresses on the

private network are not visible from the Internet, the security policy on the FortiGate unit that accepts SIP sessions includes a virtual IP. Phone A sends SIP the INVITE message to the virtual IP address. The FortiGate unit accepts the INVITE message packets and using the virtual IP, translates the destination address of the packet to the IP address of the SIP proxy server and forwards the SIP message to it.

SIP destination NAT scenario part 1: INVITE request sent from Phone B to Phone A



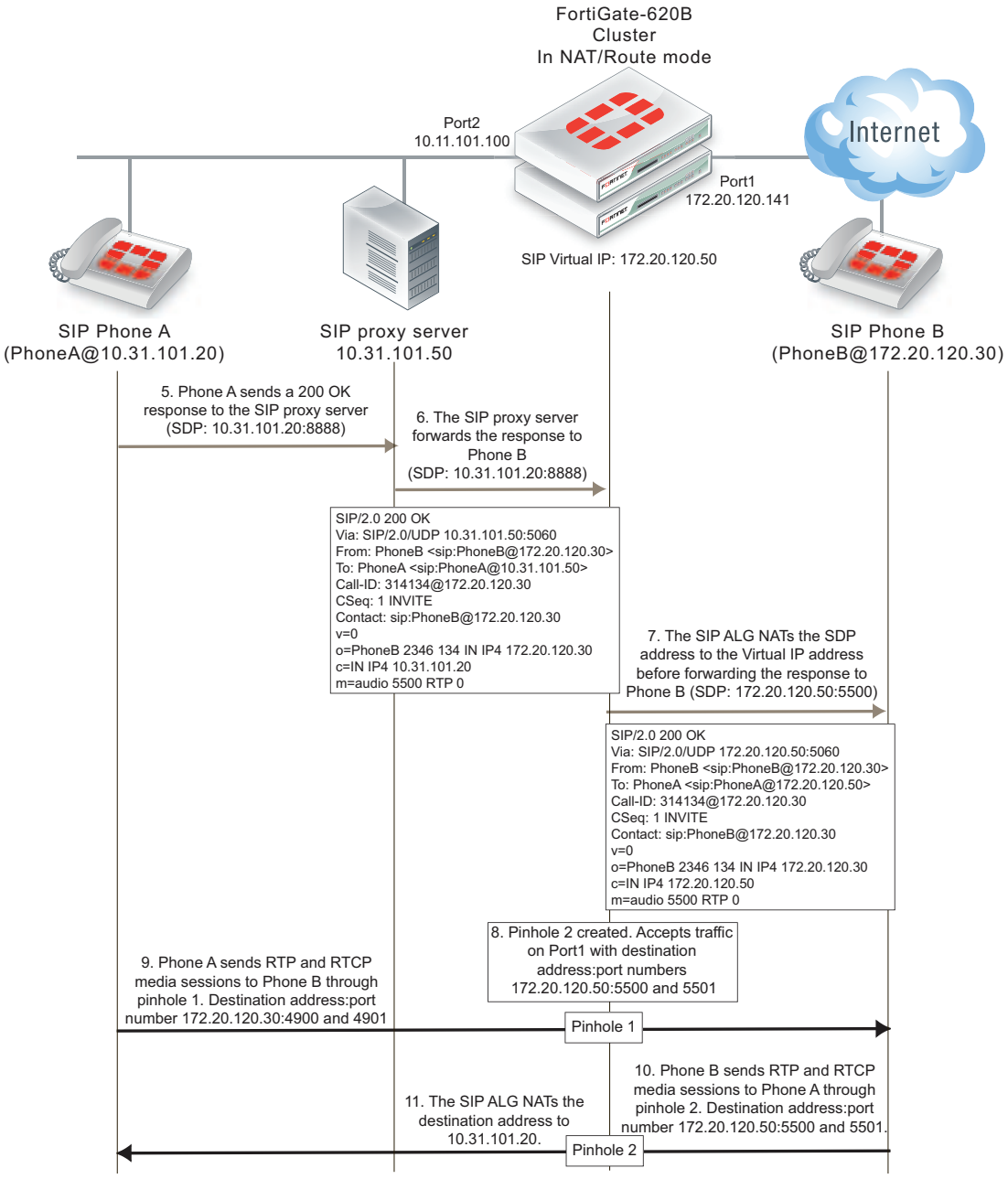
To simplify the diagrams, some SIP messages are not included (for example, the Ringing and ACK response messages) and some SIP header lines and SDP profile lines have been removed from the SIP messages.

The SIP ALG also translates the destination addresses in the SIP message from the virtual IP address (172.20.120.50) to the SIP proxy server address (10.31.101.50). For this configuration to work, the SIP proxy server must be able to change the destination addresses for Phone A in the SIP message from the address of the SIP proxy server to the actual address of Phone A.

The SIP ALG also opens a pinhole on the Port2 interface that accepts media sessions from the private network to SIP Phone B using ports 4900 and 4901.

Phone A sends a 200 OK response back to the SIP proxy server. The SIP proxy server forwards the response to Phone B. The FortiGate unit accepts the 100 OK response. The SIP ALG translates the Phone A addresses back to the SIP proxy server virtual IP address before forwarding the response back to Phone B. The SIP ALG also opens a pinhole using the SIP proxy server virtual IP which is the address in the o= line of the SDP profile and the port number in the m= line of the SDP code.

SIP destination NAT scenario part 2: 200 OK returned to Phone B and media streams established

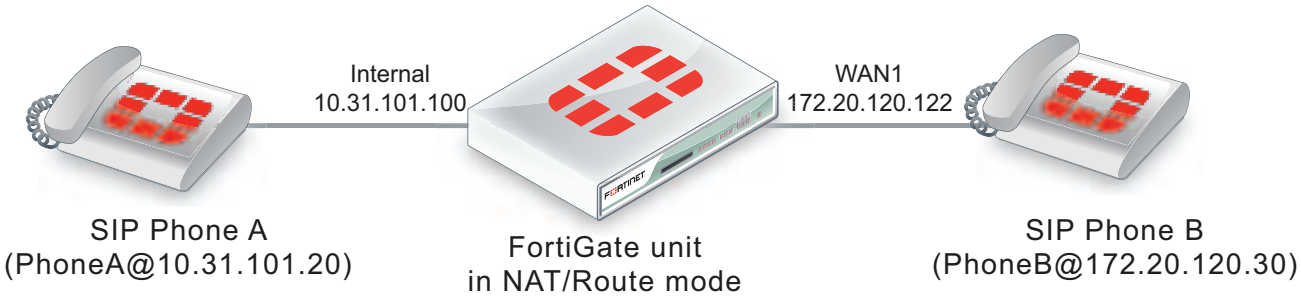


The media stream from Phone A is accepted by pinhole one and forwarded to Phone B. The source address of this media stream is changed to the SIP proxy server virtual IP address. The media stream from Phone B is accepted by pinhole 2 and forwarded to Phone B. The destination address of this media stream is changed to the IP address of Phone A.

SIP NAT configuration example: source address translation (source NAT)

This configuration example shows how to configure the FortiGate unit to support the source address translation scenario shownbelow. The FortiGate unit requires two security policies that accept SIP packets. One to allow SIP Phone A to start a session with SIP Phone B and one to allow SIP Phone B to start a session with SIP Phone A. Both of these policies must include source NAT. In this example the networks are not hidden from each other so destination NAT is not required.

SIP source NAT configuration



General configuration steps

The following general configuration steps are required for this SIP configuration. This example uses the default VoIP profile. The example also includes security policies that specifically allow SIP sessions using UDP port 5060 from Phone A to Phone B and from Phone B to Phone A. In most cases you would have more than two phones so would use more general security policies. Also, you can set the firewall service to ANY to allow traffic other than SIP on UDP port 5060.

1. Add firewall addresses for Phone A and Phone B.
2. Add a security policy that accepts SIP sessions initiated by Phone A and includes the default VoIP profile.
3. Add a security policy that accepts SIP sessions initiated by Phone B and includes the default VoIP profile.

Configuration steps - web-based manager

To add firewall addresses for the SIP phones

1. Go to **Policy & Objects > Objects > Addresses**.
2. Add the following addresses for Phone A and Phone B:

Category	Address
Name	Phone_A
Type	Subnet
Subnet / IP Range	10.31.101.20/255.255.255.255
Interface	Internal

Category	Address
Name	Phone_B
Type	Subnet
Subnet / IP Range	172.20.120.30/255.255.255.255
Interface	wan1

To add security policies to apply the SIP ALG to SIP sessions

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New** to add a security policy.
3. Add a security policy to allow Phone A to send SIP request messages to Phone B:

Incoming Interface	internal
Source Address	Phone_A
Outgoing Interface	wan1
Destination Address	Phone_B
Schedule	always
Service	SIP
Action	ACCEPT

4. Select **Enable NAT** and select **Use Destination Interface Address**.
5. Turn on **VoIP** and select the **default** VoIP profile.
6. Select **OK**.
7. Add a security policy to allow Phone B to send SIP request messages to Phone A:

Incoming Interface	wan1
Source Address	Phone_B
Outgoing Interface	internal
Destination Address	Phone_A
Schedule	always
Service	SIP
Action	ACCEPT

8. Select **Enable NAT** and select **Use Destination Interface Address**.
9. Turn on **VoIP** and select the **default** VoIP profile.
10. Select **OK**.

Configuration steps - CLI

To add firewall addresses for Phone A and Phone B and security policies to apply the SIP ALG to SIP sessions

1. Enter the following command to add firewall addresses for Phone A and Phone B.

```
config firewall address
   edit Phone_A
      set associated interface internal
      set type ipmask
      set subnet 10.31.101.20 255.255.255.255
   next
   edit Phone_B
      set associated interface wan1
      set type ipmask
      set subnet 172.20.120.30 255.255.255.255
   end
```

2. Enter the following command to add security policies to allow Phone A to send SIP request messages to Phone B and Phone B to send SIP request messages to Phone A.

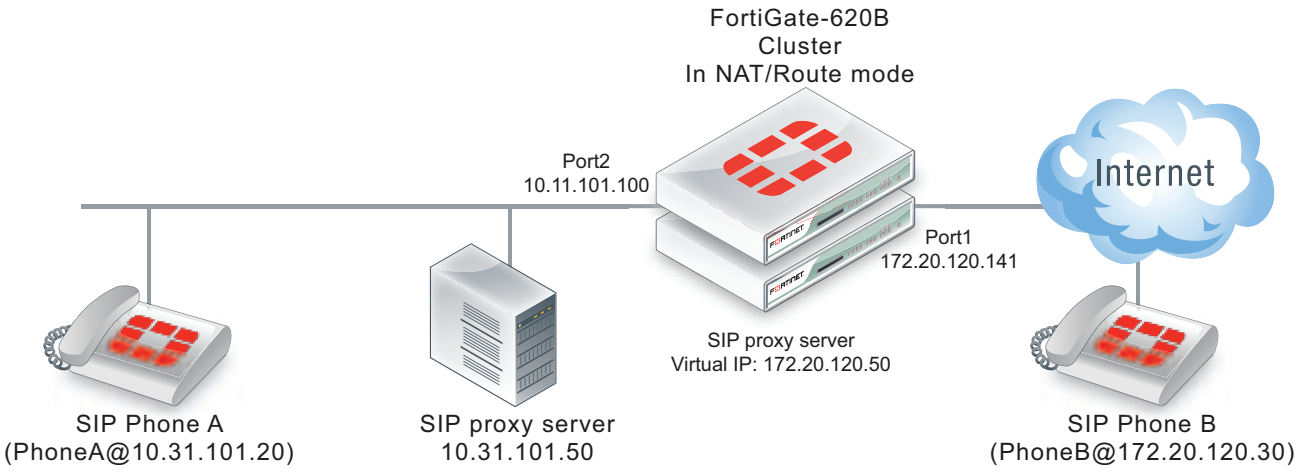
```
config firewall policy
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr Phone_A
      set dstaddr Phone_B
      set action accept
      set schedule always
      set service SIP
      set nat enable
      set utm-status enable
      set voip-profile default
   next
   edit 0
      set srcintf wan1
      set dstintf internal
      set srcaddr Phone_B
      set dstaddr Phone_A
      set action accept
      set schedule always
      set service SIP
      set nat enable
      set utm-status enable
      set voip-profile default
   end
```

SIP NAT configuration example: destination address translation (destination NAT)

This configuration example shows how to configure the FortiGate unit to support the destination address translation scenario shown in the figure below. The FortiGate unit requires two SIP security policies:

- A destination NAT security policy that allows SIP messages to be sent from the Internet to the private network. This policy must include destination NAT because the addresses on the private network are not routable on the Internet.
- A source NAT security policy that allows SIP messages to be sent from the private network to the Internet.

SIP destination NAT scenario part two: 200 OK returned to Phone B and media streams established



General configuration steps

The following general configuration steps are required for this destination NAT SIP configuration. This example uses the default VoIP profile.

1. Add the SIP proxy server firewall virtual IP.
2. Add a firewall address for the SIP proxy server on the private network.
3. Add a destination NAT security policy that accepts SIP sessions from the Internet destined for the SIP proxy server virtual IP and translates the destination address to the IP address of the SIP proxy server on the private network.
4. Add a security policy that accepts SIP sessions initiated by the SIP proxy server and destined for the Internet.

Configuration steps - web-based manager

To add the SIP proxy server firewall virtual IP

1. Go to **Policy & Objects > Objects > Virtual IP** and select **Create New**.
2. Add the SIP proxy server virtual IP.

VIP Type	IPv4 VIP
Name	SIP_Proxy_VIP
Interface	port1
Type	Static NAT
External IP Address/Range	172.20.120.50
Mapped IP Address/Range	10.31.101.50

To add a firewall address for the SIP proxy server

1. Go to **Firewall Objects > Address > Addresses**.
2. Add the following for the SIP proxy server:

To add the security policies

1. Go to **Policy & Objects > Policy > IPv4**.
2. Add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

Incoming Interface	port1
Source Address	all
Outgoing Interface	port2
Destination Address	SIP_Proxy_VIP
Schedule	always
Service	SIP
Action	ACCEPT

3. Select **Enable NAT** and select **Use Destination Interface Address**.
4. Under **UTM Security Profiles**, select **Use Standard UTM Profiles**.
5. Turn on **VoIP** and select the **default** VoIP profile.
6. Select **OK**.
7. Add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

Incoming Interface	port2
Source Address	SIP_Proxy_Server
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	SIP
Action	ACCEPT

8. Select **Enable NAT** and select **Use Destination Interface Address**.
9. Turn on **VoIP** and select the **default** VoIP profile.
10. Select **OK**.

Configuration steps - CLI

To add the SIP proxy server firewall virtual IP and firewall address

1. Enter the following command to add the SIP proxy server firewall virtual IP.

```
config firewall vip
  edit SIP_Proxy_VIP
```

```
      set type static-nat
      set extip 172.20.120.50
      set mappedip 10.31.101.50
      set extintf port1
   end
```

2. Enter the following command to add the SIP proxy server firewall address.

```
config firewall address
   edit SIP_Proxy_Server
      set associated interface port2
      set type ipmask
      set subnet 10.31.101.50 255.255.255.255
   end
```

To add security policies

1. Enter the following command to add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr all
      set dstaddr SIP_Proxy_VIP
      set action accept
      set schedule always
      set service SIP
      set nat enable
      set utm-status enable
      set voip-profile default
   end
```

2. Enter the following command to add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr SIP_Proxy_Server
      set dstaddr all
      set action accept
      set schedule always
      set service SIP
      set nat enable
      set utm-status enable
      set voip-profile default
   end
```

Additional SIP NAT scenarios

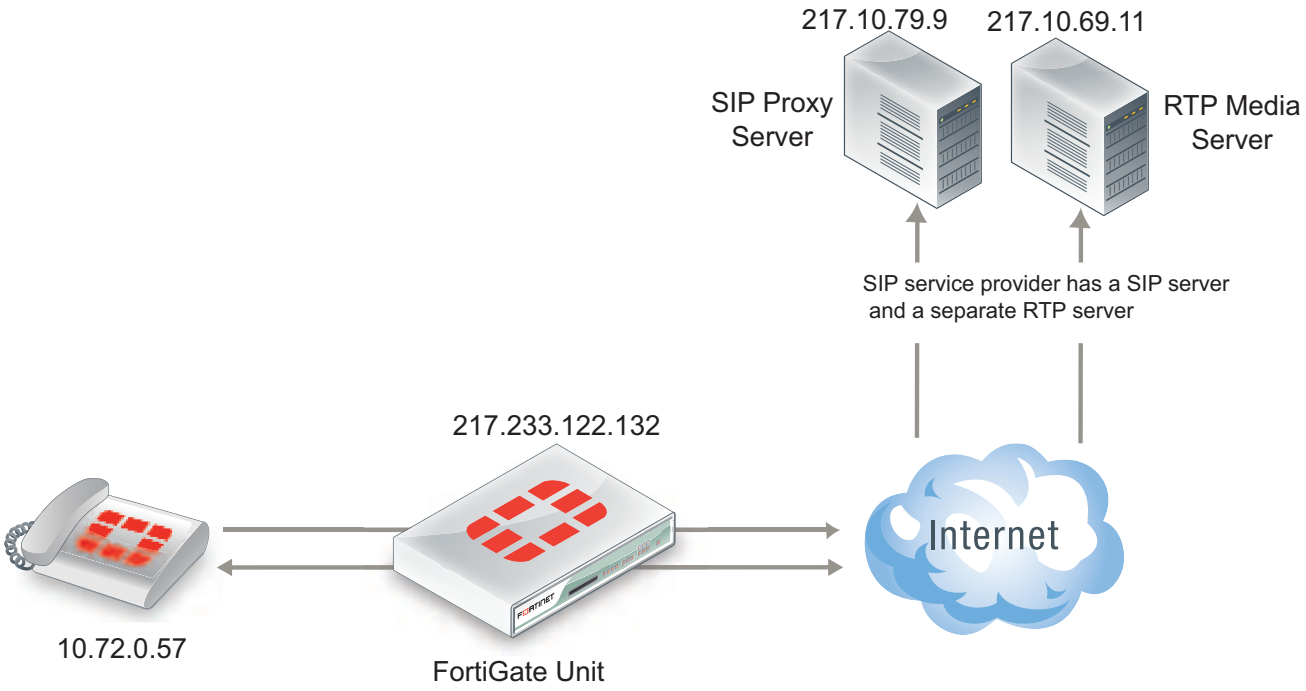
This section lists some additional SIP NAT scenarios.

Source NAT (SIP and RTP)

In the source NAT scenario shown below, a SIP phone connects to the Internet through a FortiGate unit with and IP address configured using PPPoE. The SIP ALG translates all private IPs in the SIP contact header into public IPs.

You need to configure an internal to external SIP security policy with NAT selected, and include a VoIP profile with SIP enabled.

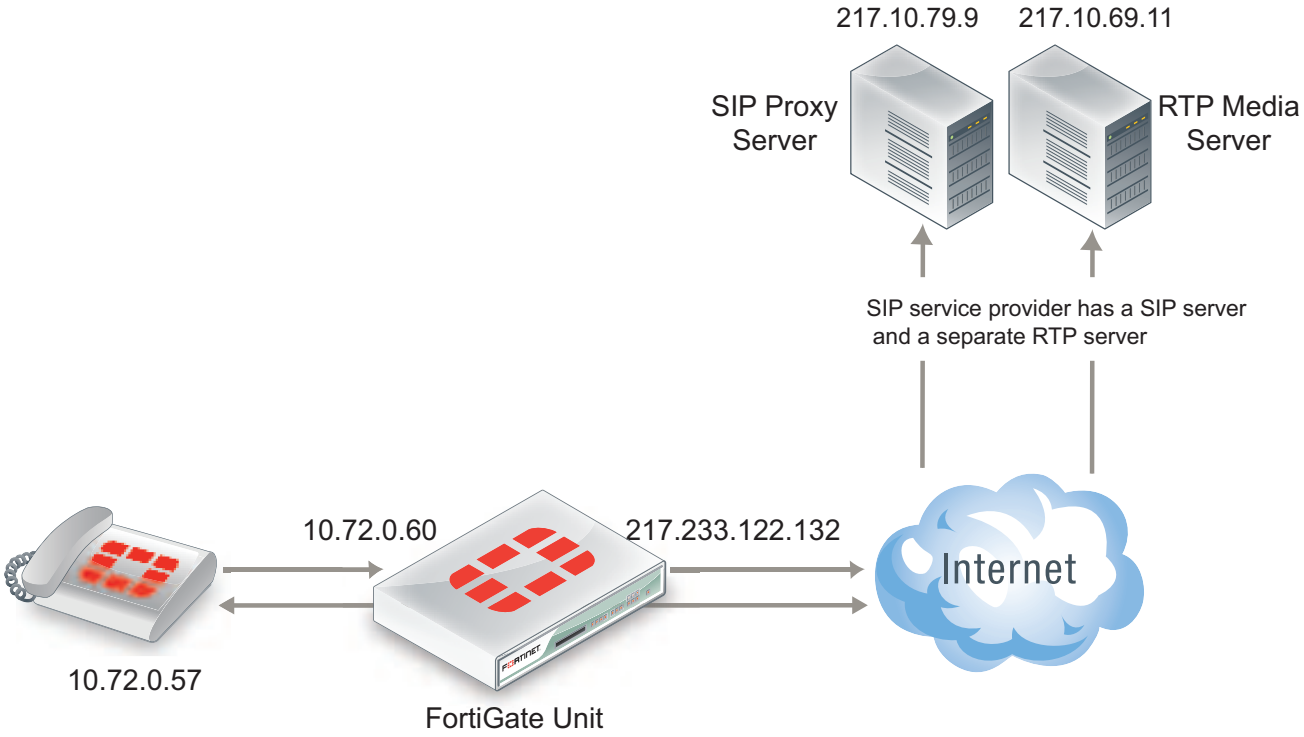
SIP source NAT



Destination NAT (SIP and RTP)

In the following destination NAT scenario, a SIP phone can connect through the FortiGate unit to private IP address using a firewall virtual IP (VIP). The SIP ALG translates the SIP contact header to the IP of the real SIP proxy server located on the Internet.

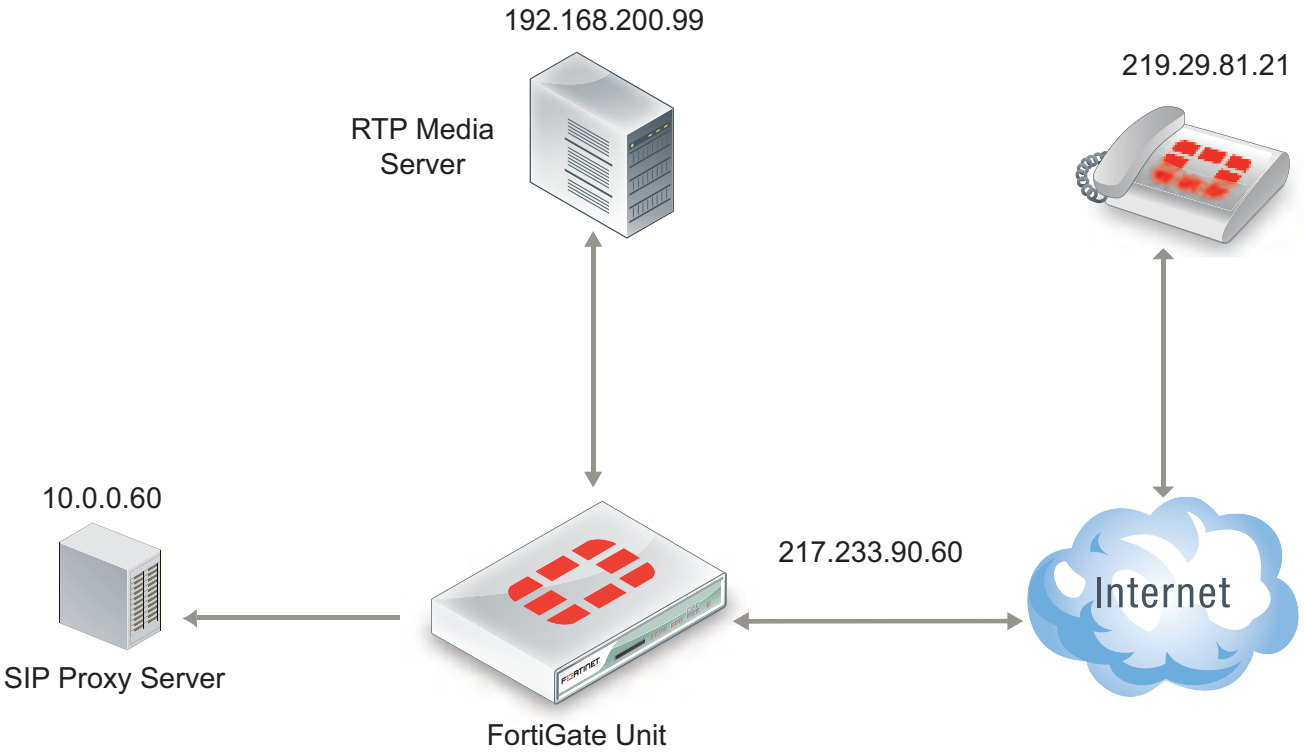
SIP destination NAT



In the scenario, shownabove, the SIP phone connects to a VIP (10.72.0.60). The SIP ALG translates the SIP contact header to 217.10.79.9, opens RTP pinholes, and manages NAT.

The FortiGate unit also supports a variation of this scenario where the RTP media server's IP address is hidden on a private network or DMZ.

SIP destination NAT-RTP media server hidden



In the scenario shown above, a SIP phone connects to the Internet. The VoIP service provider only publishes a single public IP. The FortiGate unit is configured with a firewall VIP. The SIP phone connects to the FortiGate unit (217.233.90.60) and using the VIP the FortiGate unit translates the SIP contact header to the SIP proxy server IP address (10.0.0.60). The SIP proxy server changes the SIP/SDP connection information (which tells the SIP phone which RTP media server IP it should contact) also to 217.233.90.60.

Source NAT with an IP pool

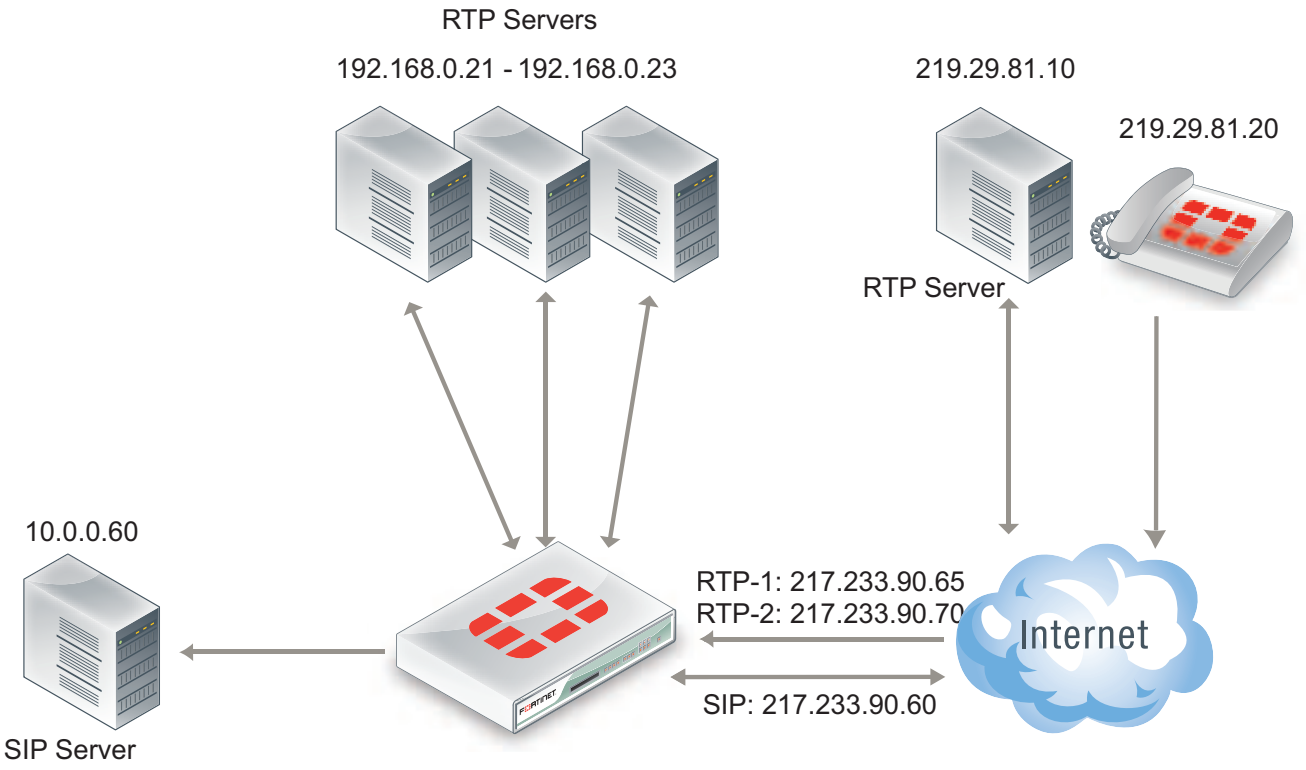
You can choose **NAT** with the **Dynamic IP Pool** option when configuring a security policy if the source IP of the SIP packets is different from the interface IP. The FortiGate ALG interprets this configuration and translates the SIP header accordingly.

This configuration also applies to destination NAT.

Different source and destination NAT for SIP and RTP

This is a more complex scenario that a SIP service provider may use. It can also be deployed in large-scale SIP environments where RTP has to be processed by the FortiGate unit and the RTP server IP has to be translated differently than the SIP serverIP.

Different source and destination NAT for SIP and RTP



In this scenario, shown above, assume there is a SIP server and a separate media gateway. The SIP server is configured so that the SIP phone (219.29.81.20) will connect to 217.233.90.60. The media gateway (RTP server: 219.29.81.10) will connect to 217.233.90.65.

What happens is as follows:

1. The SIP phone connects to the SIP VIP. The FortiGate ALG translates the SIP contact header to the SIP server: 219.29.81.20 > 217.233.90.60 (> 10.0.0.60).
2. The SIP server carries out RTP to 217.233.90.65.
3. The FortiGate ALG opens pinholes, assuming that it knows the ports to be opened.
4. RTP is sent to the RTP-VIP (217.233.90.65.) The FortiGate ALG translates the SIP contact header to 192.168.0.21.

NAT with IP address conservation

In a source or destination NAT security policy that accepts SIP sessions, you can configure the SIP ALG or the SIP session helper to preserve the original source IP address of the SIP message in the i= line of the SDP profile. NAT with IP address conservation (also called SIP NAT tracing) changes the contents of SIP messages by adding the source IP address of the originator of the message into the SDP i= line of the SIP message. The SDP i= line is used for free-form text. However, if your SIP server can retrieve information from the SDP i= line, it can be useful for keeping a record of the source IP address of the originator of a SIP message when operating in a NAT environment. You can use this feature for billing purposes by extracting the IP address of the originator of the message.

Configuring SIP IP address conservation for the SIP ALG

You can use the following command to enable or disable SIP IP address conservation in a VoIP profile for the SIP ALG. SIP IP address conservation is enabled by default in a VoIP profile.

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set nat-trace disable
      end
   end
```

If the SIP message does not include an i= line and if the original source IP address of the traffic (before NAT) was 10.31.101.20 then the FortiGate unit would add the following i= line.

```
i=(o=IN IP4 10.31.101.20)
```

You can also use the `preserve-override` option to configure the SIP ALG to either add the original o= line to the end of the i= line or replace the i= line in the original message with a new i= line in the same form as above for adding a new i= line.

By default, `preserver-override` is disabled and the SIP ALG adds the original o= line to the end of the original i= line. Use the following command to configure the SIP ALG to replace the original i= line:

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set preserve-override enable
      end
   end
```

Configuring SIP IP address conservation for the SIP session helper

You can use the following command to enable or disable SIP IP address conservation for the SIP session helper. IP address conservation is enabled by default for the SIP session helper.

```
config system settings
   set sip-nat-trace disable
end
```

If the SIP message does not include an i= line and if the original source IP address of the traffic (before NAT) was 10.31.101.20 then the FortiGate unit would add the following i= line.

```
i=(o=IN IP4 10.31.101.20)
```

Controlling how the SIP ALG NATs SIP contact header line addresses

You can enable `contact-fixup` so that the SIP ALG performs normal SIP NAT translation to SIP contact headers as SIP messages pass through the FortiGate unit.

Disable `contact-fixup` if you do not want the SIP ALG to perform normal NAT translation of the SIP contact header if a Record-Route header is also available. If `contact-fixup` is disabled, the FortiGate ALG does the following with contact headers:

- For Contact in Requests, if a Record-Route header is present and the request comes from the external network, the SIP Contact header is not translated.
- For Contact in Responses, if a Record-Route header is present and the response comes from the external network, the SIP Contact header is not translated.

If `contact-fixup` is disabled, the SIP ALG must be able to identify the external network. To identify the external network, you must use the `config system interface` command to set the `external` keyword to `enable` for the interface that is connected to the external network.

Enter the following command to perform normal NAT translation of the SIP contact header:

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set contact-fixup enable
      end
   end
```

Controlling NAT for addresses in SDP lines

You can use the `no-sdp-fixup` option to control whether the FortiGate unit performs NAT on addresses in SDP lines in the SIP message body.

The `no-sdp-fixup` option is disabled by default and the FortiGate unit performs NAT on addresses in SDP lines. Enable this option if you don't want the FortiGate unit to perform NAT on the addresses in SDP lines.

```
config voip profile
   edit VoIP_Pro_1
      config sip
         set no-sdp-fixup enable
      end
   end
```

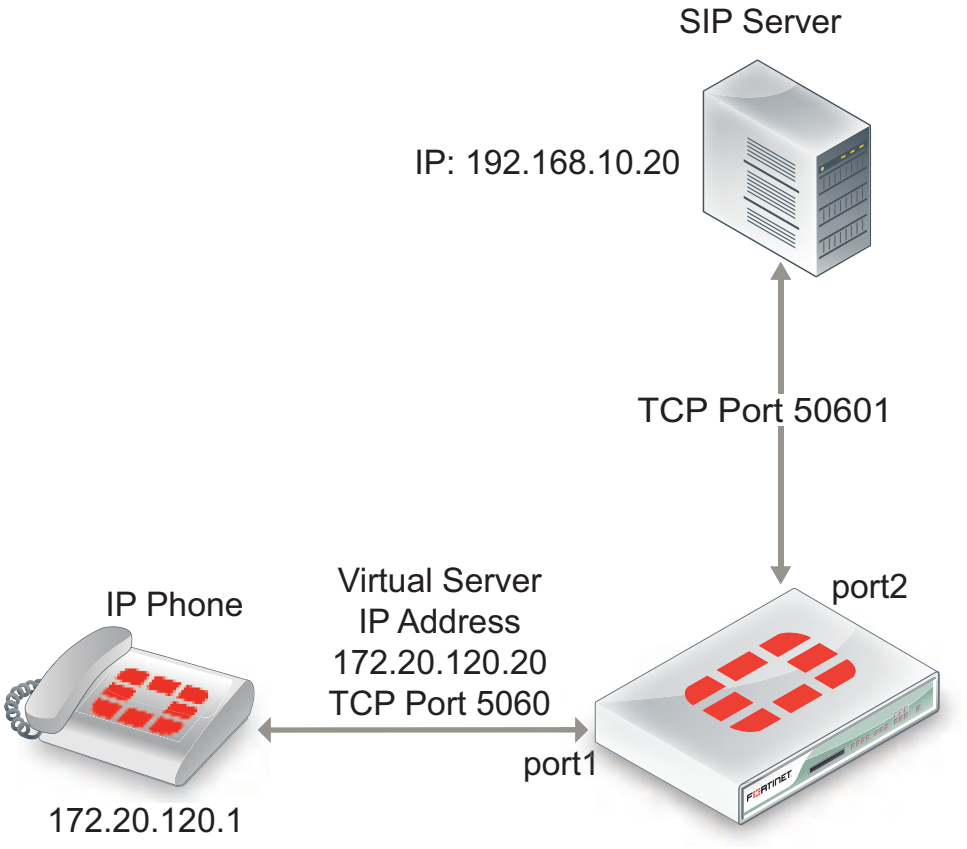
Translating SIP session destination ports

Using port forwarding virtual IPs you can change the destination port of SIP sessions as they pass through the FortiGate unit.

Translating SIP sessions to a different destination port

To configure translating SIP sessions to a different destination port you must add a static NAT virtual IP that translates tie SIP destination port to another port destination. In the example the destination port is translated from 5060 to 50601. This configuration can be used if SIP sessions uses different destination ports on different networks.

Example translating SIP sessions to a different destination port



To translate SIP sessions to a different destination port

1. Add the static NAT virtual IP.

   This virtual IP forwards traffic received at the port1 interface for IP address 172.20.120.20 and destination port 5060 to the SIP server at IP address 192.168.10.20 with destination port 5061.

```
config firewall vip
   edit "sip_port_trans_vip"
      set type static-nat
      set portforward enable
      set protocol tcp
      set extip 172.20.120.20
      set extport 5060
      set extintf "port1"
      set mappedip 192.168.10.20
      set mappedport 50601
      set comment "Translate SIP destination port"
   end
```

2. Add a security policy that includes the virtual IP and the default VoIP profile.

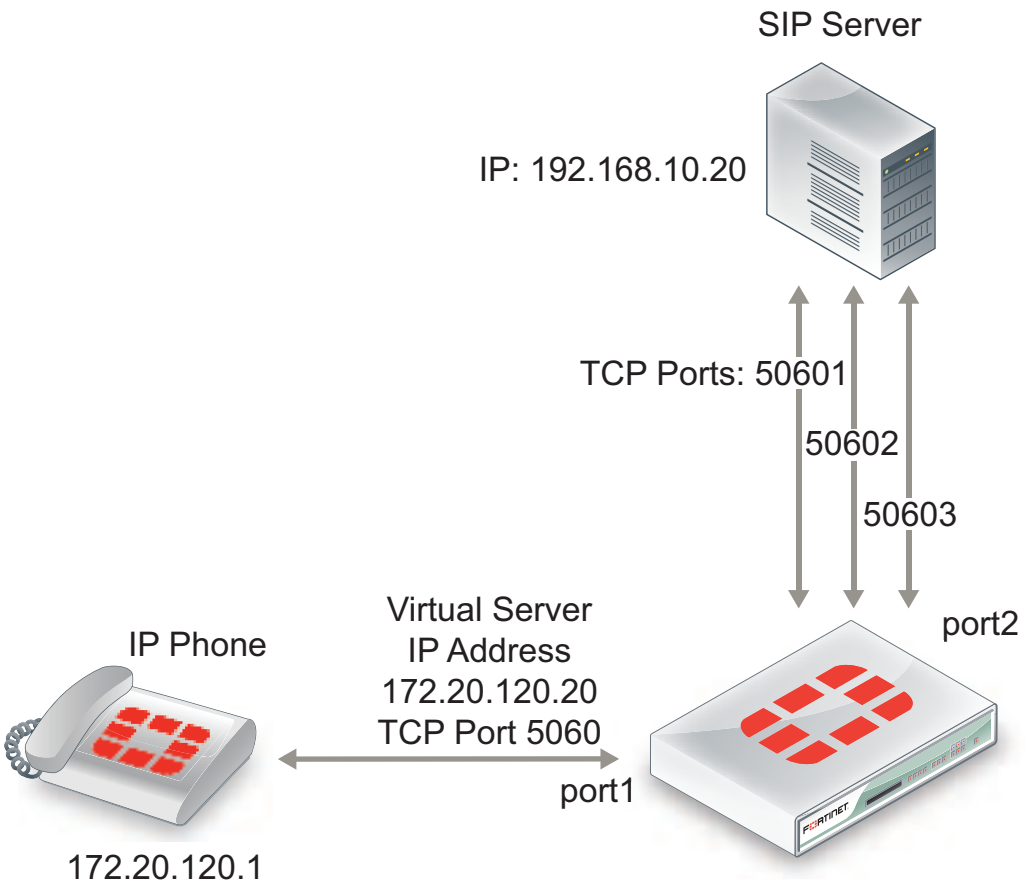
```
config firewall policy
   edit 1
      set srcintf "port1"
```

```
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "sip_port_trans_vip"
    set action accept
    set schedule "always"
    set service "ANY"
    set utm-status enable
    set profile-protocol-options default
    set comments "Translate SIP destination port"
end
```

Translating SIP sessions to multiple destination ports

You can use a load balance virtual IP to translate SIP session destination ports to a range of destination ports. In this example the destination port is translated from 5060 to the range 50601 to 50603. This configuration can be used if your SIP server is configured to receive SIP traffic on multiple ports.

Example translating SIP traffic to multiple destination ports



To translated SIP sessions to multiple destination ports

1. Add the load balance virtual IP.

   This virtual IP forwards traffic received at the port1 interface for IP address 172.20.120.20 and destination port 5060 to the SIP server at IP address 192.168.10.20 with destination port 5061.

```
config firewall vip
   edit "sip_port_ldbl_vip"
      set type load-balance
      set portforward enable
      set protocol tcp
      set extip 172.20.120.20
      set extport 5060
      set extintf "port1"
      set mappedip 192.168.10.20
      set mappedport 50601-50603
      set comment "Translate SIP destination port range"
   end
```

2. Add a security policy that includes the virtual IP and VoIP profile.

```
config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "all"
      set dstaddr "sip_port_ldbl_vip"
      set action accept
      set schedule "always"
      set service "ANY"
      set utm-status enable
      set voip-profile default
      set comments "Translate SIP destination port"
   end
```

Adding the original IP address and port to the SIP message header after NAT

In some cases your SIP configuration may require that the original IP address and port from the SIP contact request is kept after NAT. For example, the original SIP contact request could include the following:

```
Contact: <sip:0150302438@172.20.120.110:5060>;
```

After the packet goes through the FortiGate unit and NAT is performed, the contact request could normally look like the following (the IP address translated to a different IP address and the port to a different port):

```
Contact: <sip:0150302438@10.10.10.21:33608>;
```

You can enable `register-contact-trace` in a VoIP profile to have the SIP ALG add the original IP address and port in the following format:

```
Contact: <sip:0150302438@<nated-ip>:<nated-port>;o=<original-ip>: <original-port>>;
```

So the contact line after NAT could look like the following:

```
Contact: <sip:0150302438@10.10.10.21:33608;o=172.20.120.110:5060>;
```

Enter the following command to enable keeping the original IP address and port:

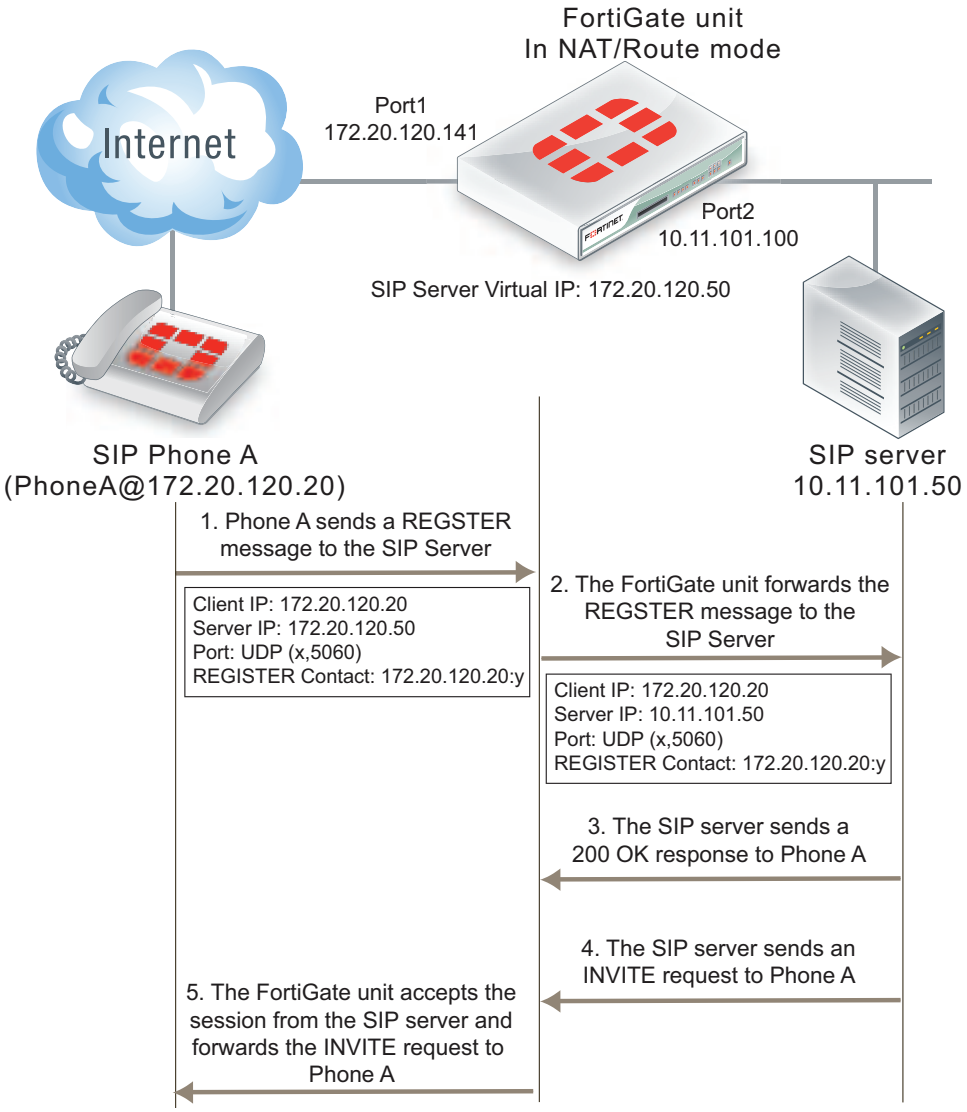
```
config voip profile
   edit Profile_name
      config sip
         set register-contract-trace enable
   end
```

Enhancing SIP pinhole security

You can use the `strict-register` option in a SIP VoIP profile to open smaller pinholes.

As shown below, when FortiGate unit is protecting a SIP server on a private network, the FortiGate unit does not have to open a pinhole for the SIP server to send INVITE requests to a SIP Phone on the Internet after the SIP Phone has registered with the server.

FortiGate unit protecting a SIP server on a private network



In the example, a client (SIP Phone A) sends a REGISTER request to the SIP server with the following information:

```
Client IP: 10.31.101.20
Server IP: 10.21.101.50
Port: UDP (x,5060)
REGISTER Contact: 10.31.101.20:y
```

Where `x` and `y` are ports chosen by Phone A.

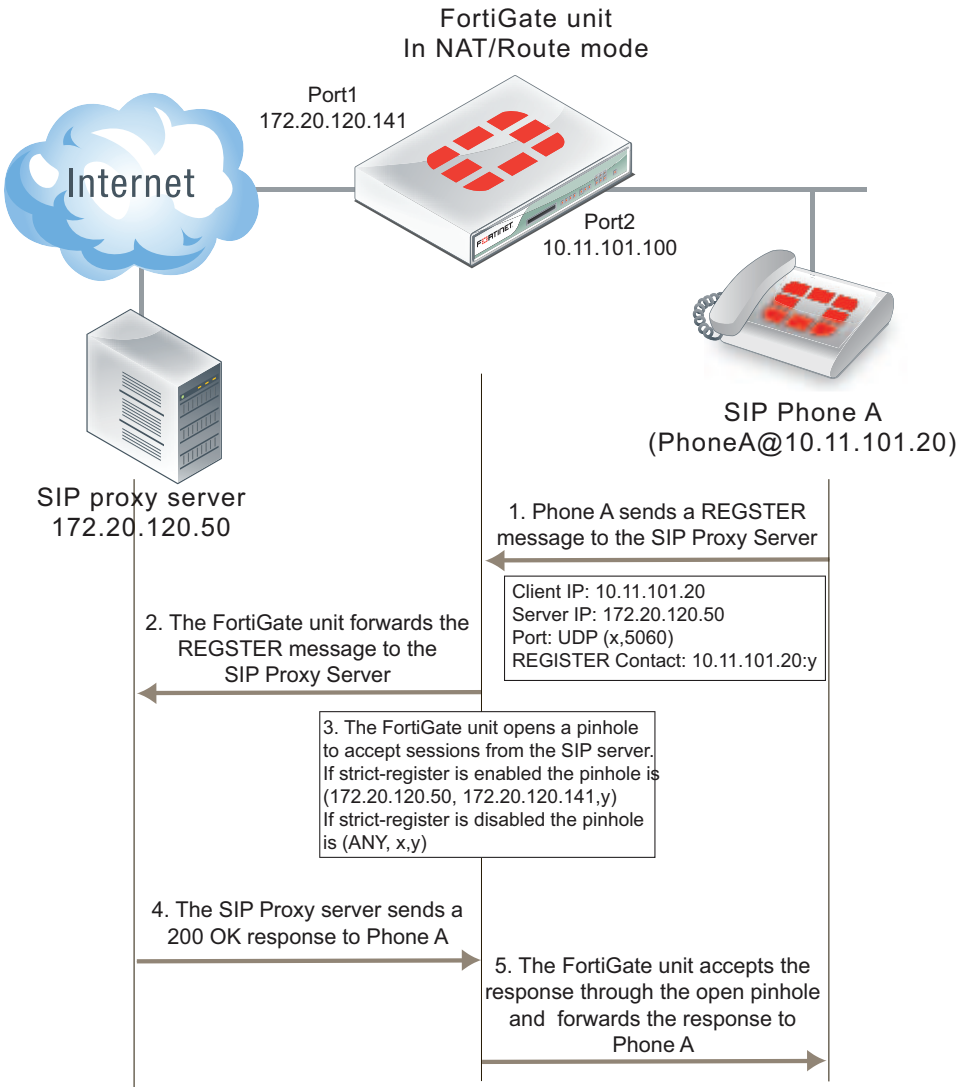
As soon as the server sends the 200 OK reply it can forward INVITE requests from other SIP phones to SIP Phone A. If the SIP proxy server uses the information in the REGISTER message received from SIP Phone A the INVITE messages sent to Phone A f will only get through the FortiGate unit if an policy has been added to allow the

server to send traffic from the private network to the Internet. Or the SIP ALG must open a pinhole to allow traffic from the server to the Internet. In most cases the FortiGate unit is protecting the SIP server so there is no reason not to add a security policy to all the SIP server to send outbound traffic to the Internet.

In a typical SOHO scenario, shown below, SIP Phone A is being protected from the Internet by a FortiGate unit. In most cases the FortiGate unit would not allow incoming traffic from the Internet to reach the private network. So the only way that an INVITE request from the SIP server can reach SIP Phone A is if the SIP ALG creates an incoming pinhole. All pinholes have three attributes:

```
(source address, destination address, destination port)
```

SOHO configuration, FortiGate unit protecting a network with SIP phones



The more specific a pinhole is the more secure it is because it will accept less traffic. In this situation, the pinhole would be more secure if it only accepted traffic from the SIP server. This is what happens if `strict-register` is enabled in the VoIP profile that accepts the REGISTER request from Phone A.

```
(SIP server IP address, client IP address, destination port)
```

If `strict-register` is disabled (the default configuration) the pinhole is set up with the following attributes

```
(ANY IP address, client IP address, destination port)
```

This pinhole allows connections through the FortiGate unit from ANY source address which is a much bigger and less secure pinhole. In most similar network configurations you should enable `strict-register` to improve pinhole security.

Enabling `strict-register` can cause problems when the SIP registrar and SIP proxy server are separate entities with separate IP addresses.

Enter the following command to enable `strict-register` in a VoIP profile.

```
config voip profile
   edit Profile_name
      config sip
         set strict-register enable
   end
```

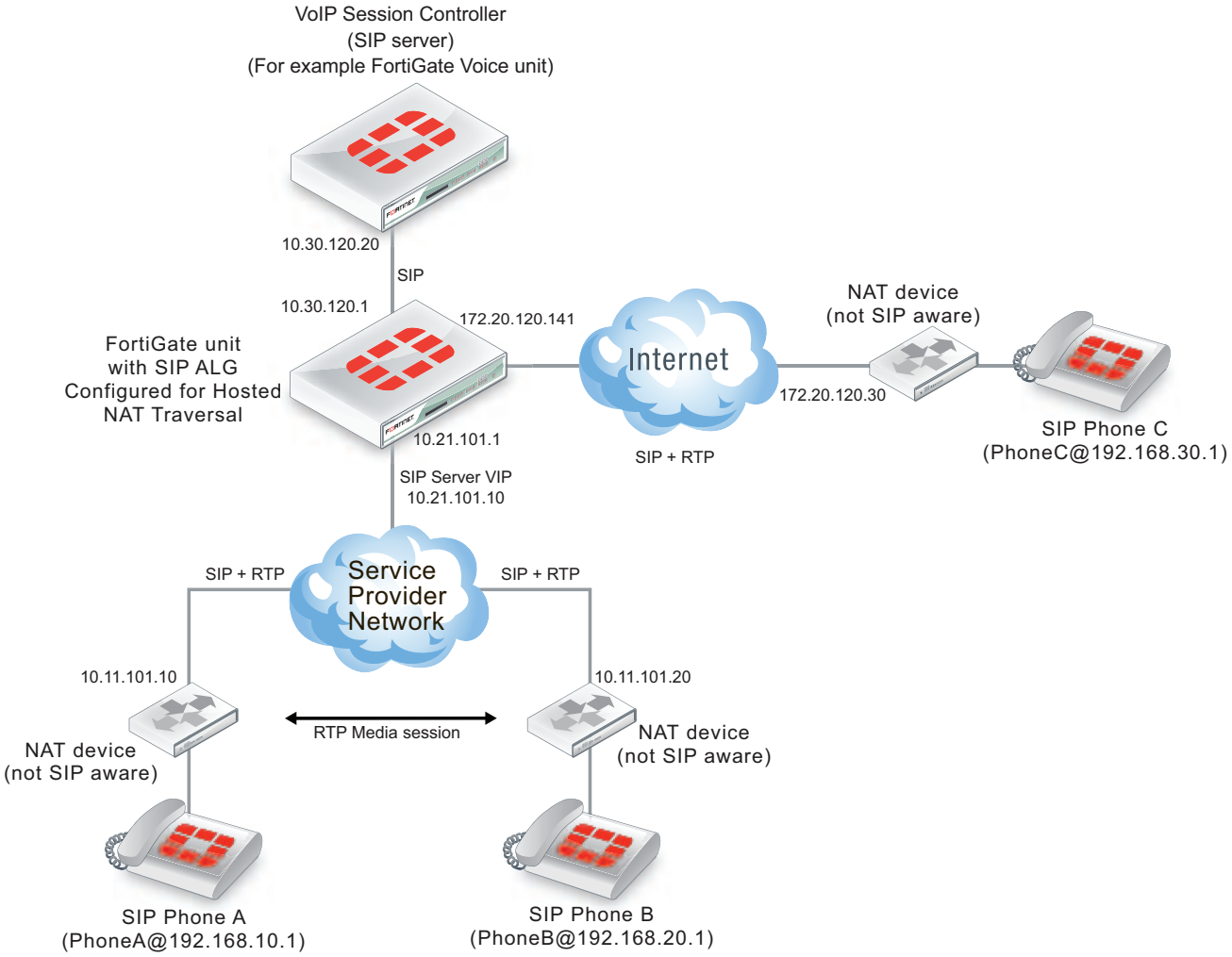
Hosted NAT traversal

With the increase in the use of VoIP and other media traffic over the Internet, service provider network administrators must defend their networks from threats while allowing voice and multimedia traffic to flow transparently between users and servers and among users. A common scenario could involve providing SIP VoIP services for customers with SIP phones installed behind NAT devices that are not SIP aware. NAT devices that are not SIP aware cannot translate IP addresses in SIP headers and SDP lines in SIP packets but can and do perform source NAT on the source or addresses of the packets. In this scenario the user's SIP phones would communicate with a SIP proxy server to set up calls between SIP phones. Once the calls are set up RTP packets would be communicated directly between the phones through each user's NAT device.

The problem with this configuration is that the SIP headers and SDP lines in the SIP packets sent from the phones and received by the SIP proxy server would contain the private network addresses of the VoIP phones that would not be routable on the service provider network or on the Internet. One solution could be to for each customer to install and configure SIP aware NAT devices. If this is not possible, another solution requires implement hosted NAT traversal.

In a hosted NAT traversal (HNT) configuration, a FortiGate unit is installed between the NAT device and the SIP proxy server and configured with a VoIP profile that enables SIP hosted NAT traversal. Security policies that include the VoIP profile also support destination NAT using a firewall virtual IP. When the SIP phones connect to the SIP server IP address the security policy accepts the SIP packets, the virtual IP translates the destination addresses of the packets to the SIP server IP address, and the SIP ALG NAT traversal configuration translates the source IP addresses on the SIP headers and SDP lines to the source address of the SIP packets (which would be the external IP address of the NAT devices). The SIP server then sees the SIP phone IP address as the external IP address of the NAT device. As a result SIP and RTP media sessions are established using the external IP addresses of the NAT devices instead of the actual IP addresses of the SIP phones.

FortiGate SIP Hosted NAT Traversal configuration



Configuration example: Hosted NAT traversal for calls between SIP Phone A and SIP Phone B

The following address translation takes place to allow a SIP call from SIP Phone A to SIP Phone B in the above diagram.

1. SIP Phone A sends a SIP Invite message to the SIP server. Packet source IP address: 192.168.10.1, destination IP address: 10.21.101.10.
2. The SIP packets are received by the NAT device which translates the source address of the SIP packets from 192.168.10.1 to 10.11.101.20.
3. The SIP packets are received by the FortiGate unit which translates the packet destination IP address to 10.30 120.20. The SIP ALG also translates the IP address of the SIP phone in the SIP header and SDP lines from 192.168.10.1 to 10.11.101.20.
4. The SIP server accepts the Invite message and forwards it to SIP Phone B at IP address10.11.101.20. The SIP server has this address for SIP Phone B because SIP packets from SIP Phone B have also been translated using the hosted NAT traversal configuration of the SIP ALG.

5. When the SIP call is established, the RTP session is between 10.11.101.10 and 10.11.101.20 and does not pass through the FortiGate unit. The NAT devices translated the destination address of the RTP packets to the private IP addresses of the SIP phones.

General configuration steps

The following general configuration steps are required for this destination NAT SIP configuration. This example uses the default VoIP profile.

1. Add a VoIP profile that enables hosted NAT translation.
2. Add a SIP proxy server firewall virtual IP.
3. Add a firewall address for the SIP proxy server on the private network.
4. Add a destination NAT security policy that accepts SIP sessions from the Internet destined for the SIP proxy server virtual IP and translates the destination address to the IP address of the SIP proxy server on the private network.
5. Add a security policy that accepts SIP sessions initiated by the SIP proxy server and destined for the Internet.

Configuration steps - web-based manager

To add the SIP proxy server firewall virtual IP

1. Go to **Firewall Objects > Objects > Virtual IPs.**
2. Add the SIP proxy server virtual IP.

Name	SIP_Proxy_VIP
External Interface	port1
Type	Static NAT
External IP Address/Range	172.20.120.50
Mapped IP Address/Range	10.31.101.50

To add a firewall address for the SIP proxy server

1. Go to **Firewall Objects > Address > Addresses**.
2. Add the following for the SIP proxy server:

Category	Address
Name	SIP_Proxy_Server
Type	Subnet
Subnet / IP Range	10.31.101.50/255.255.255.255
Interface	port2

To add the security policies

1. Go to **Policy Objects > Policy > IPv4**.
2. Add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone B (and other SIP phones on the Internet) to send SIP request messages to the SIP proxy server.

Incoming Interface	port1
Source Address	all
Outgoing Interface	port2
Destination Address	SIP_Proxy_VIP
Schedule	always
Service	SIP
Action	ACCEPT

3. Select **Enable NAT** and select **Use Destination Interface Address**.
4. Turn on **VoIP** and select the **default** VoIP profile.
5. Select **OK**.
6. Add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B and the Internet:

Incoming Interface	port2
Source Address	SIP_Proxy_Server
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	SIP
Action	ACCEPT

7. Select **Enable NAT** and select **Use Destination Interface Address**.
8. Turn on **VoIP** and select the **default** VoIP profile.
9. Select **OK**.

Configuration steps - CLI

To add a VoIP profile that enables hosted NAT translation

1. Enter the following command to add a VoIP profile named HNT that enables hosted NAT traversal. This command shows how to clone the default VoIP profile and enable hosted NAT traversal.

```
config voip profile
   clone default to HNT
```

```
edit HNT
   config sip
      set hosted-nat-traversal enable
   end
end
```

To add the SIP proxy server firewall virtual IP and firewall address

1. Enter the following command to add the SIP proxy server firewall virtual IP.

```
config firewall vip
   edit SIP_Proxy_VIP
      set type static-nat
      set extip 10.21.101.10
      set mappedip 10.30.120.20
      set extintf port1
   end
```

2. Enter the following command to add the SIP proxy server firewall address.

```
config firewall address
   edit SIP_Proxy_Server
      set associated interface port2
      set type ipmask
      set subnet 10.30.120.20 255.255.255.255
   end
```

To add security policies

1. Enter the following command to add a destination NAT security policy that includes the SIP proxy server virtual IP that allows Phone A to send SIP request messages to the SIP proxy server.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr all
      set dstaddr SIP_Proxy_VIP
      set action accept
      set schedule always
      set service SIP
      set nat enable
      set utm-status enable
      set profile-protocol-options default
      set voip-profile HNT
   end
```

2. Enter the following command to add a source NAT security policy to allow the SIP proxy server to send SIP request messages to Phone B:

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr SIP_Proxy_Server
      set dstaddr all
      set action accept
      set schedule always
      set service SIP
      set nat enable
```

```
      set utm-status enable
      set profile-protocol-options default
      set voip-profile default
   end
```

Hosted NAT traversal for calls between SIP Phone A and SIP Phone C

The following address translation takes place to allow a SIP call from SIP Phone A to SIP Phone C in the previous diagram.

1. SIP Phone A sends a SIP Invite message to the SIP server. Packet source IP address: 192.168.10.1 and destination IP address: 10.21.101.10.
2. The SIP packets are received by the NAT device which translates the source address of the SIP packets from 192.168.10.1 to 10.11.101.20.
3. The SIP packets are received by the FortiGate unit which translates the packet destination IP address to 10.30 120.20. The SIP ALG also translates the IP address of the SIP phone in the SIP header and SDP lines from 192.168.10.1 to 10.11.101.20.
4. The SIP server accepts the Invite message and forwards it to SIP Phone C at IP address 172.20.120.30. The SIP server has this address for SIP Phone C because SIP packets from SIP Phone C have also been translated using the hosted NAT traversal configuration of the SIP ALG.
5. When the SIP call is established, the RTP session is between 10.11.101.10 and 172.20.120.30. The packets pass through the FortiGate unit which performs NAT as required.

Restricting the RTP source IP

Use the following command in a VoIP profile to restrict the RTP source IP to be the same as the SIP source IP when hosted NAT traversal is enabled.

```
config voip profile
   edit VoIP_HNT
      config sip
         set hosted-nat-traversal enable
         set hnt-restrict-source-ip enable
      end
   end
```

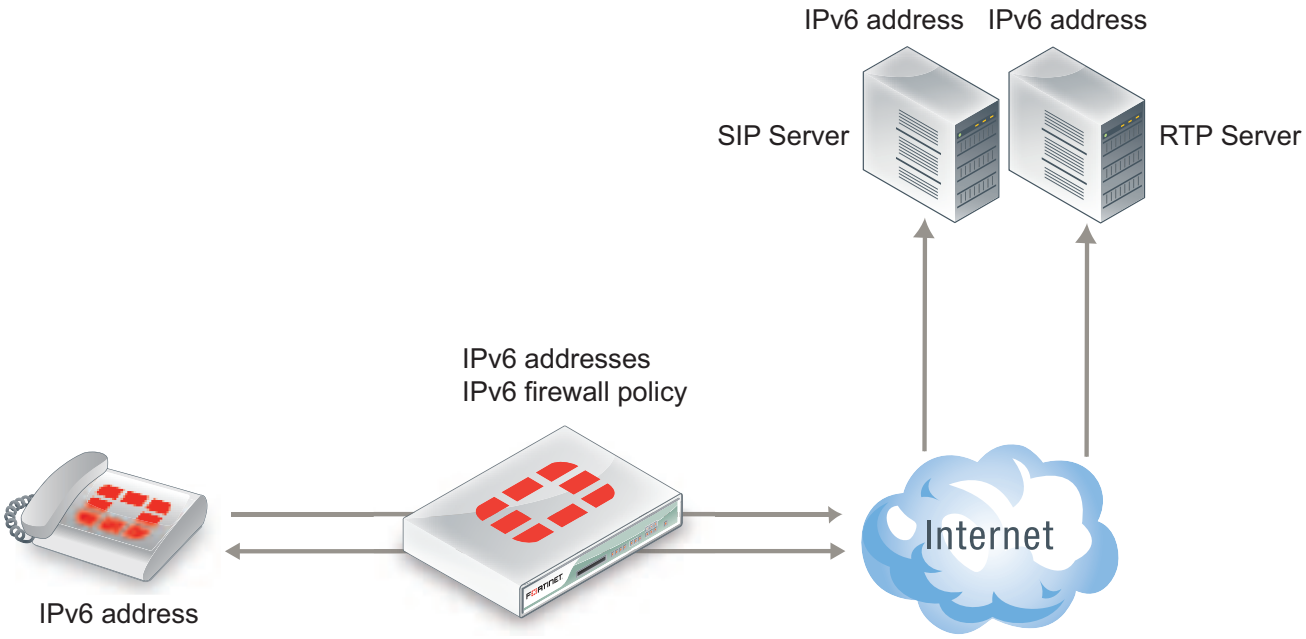
SIP over IPv6

FortiGate units operating in NAT/Route and in Transparent mode support SIP over IPv6. The SIP ALG can process SIP messages that use IPv6 addresses in the headers, bodies, and in the transport stack. The SIP ALG cannot modify the IPv6 addresses in the SIP headers so FortiGate units cannot perform SIP or RTP NAT over IPv6 and also cannot translate between IPv6 and IPv4 addresses.

In the scenario shown inthe figure below, a SIP phone connects to the Internet through a FortiGate unit operating. The phone and the SIP and RTP servers all have IPv6 addresses.

The FortiGate unit has IPv6 security policies that accept SIP sessions. The SIP ALG understands IPv6 addresses and can forward IPv6 sessions to their destinations. Using SIP application control features the SIP ALG can also apply rate limiting and other settings to SIP sessions.

SIP support for IPv6

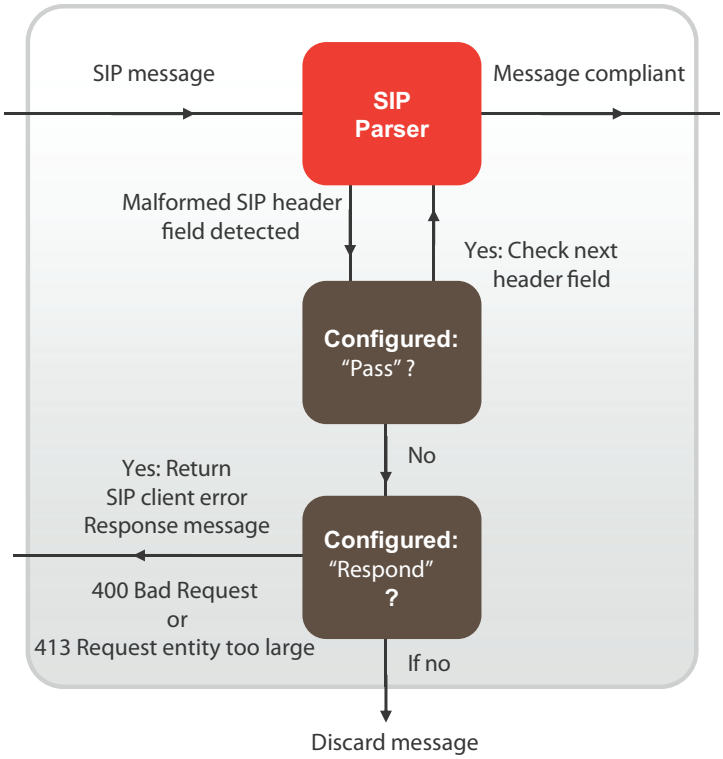


To enable SIP support for IPv6 add an IPv6 security policy that accepts SIP packets and includes a VoIP profile.

Deep SIP message inspection

Deep SIP message syntax inspection (also called Deep SIP header inspection or SIP fuzzing protection) provides protection against malicious SIP messages by applying SIP header and SDP profile syntax checking. SIP Fuzzing attacks can be used by attackers to discover and exploit vulnerabilities of a SIP entity (for example a SIP proxy server). Most often these attacks could crash or compromise the SIP entity.

Deep SIP message inspection



- **Checks the SIP request message Request-line**
- **Checks the following SIP header fields:**
  - **Allow, Call-id, Contact, Content-length, Content-type, CSeq, Expires, From, Max-Forwards, P-asserted-identity, Rack, Record-Route, Route, Rseq, To, Via**
- **Checks all SDP profile lines**
- **Configurable header and body length checks**
- **Optional logging of message violations**

Deep SIP message inspection checks the syntax of each SIP header and SDP profile line to make sure they conform to the syntax defined in the relevant RFC and IETF standard. You can also configure the SIP ALG to inspect for:

- Unknown SIP message types (message types not defined in a SIP RFC) this option is enabled by default and can be disabled. When enabled unknown message types are discarded. Configured using the `block-unknown` option.
- Unknown line types (message line types that are not defined in any SIP or SDP RFC). Configured using the `unknown-header` option.
- Messages that are longer than a configured maximum size. Configured using the `max-body-length` option.
- Messages that contain one or more lines that are longer that a set maximum line length (default 998 characters). Configured using the `max-line-length` option.

Actions taken when a malformed message line is found

When a malformed message line or other error is found the SIP ALG can be configured to discard the message containing the error, pass the message without any other actions, or responding to the message with a 400 Bad Request or 413 Request entity too large client error SIP response message and then discard the message. (For information about client error SIP response messages, see "Client error".)

If a message line is longer than the configured maximum, the SIP ALG sends the following message:

```
SIP/2.0 413 Request Entity Too Large, <optional_info>
```

If a message line is incorrect or in an unknown message line is found, the SIP ALG sends the following message:

```
SIP/2.0 400 Bad Request, <optional_info>
```

The <optional_info> provides more information about why the message was rejected. For example, if the SIP ALG finds a malformed Via header line, the response message may be:

```
SIP/2.0 400 Bad Request, malformed Via header
```

If the SIP ALG finds a malformed message line, and the action for this message line type is discard, the message is discarded with no further checking or responses. If the action is pass, the SIP ALG continues parsing the SIP message for more malformed message lines. If the action is respond, the SIP ALG sends the SIP response message and discards the message containing the malformed line with no further checking or response. If only malformed message line types with action set to pass are found, the SIP ALG extracts as much information as possible from the message (for example for NAT and opening pinholes, and forwards the message to its destination).

If a SIP message containing a malformed line is discarded the SIP ALG will not use the information in the message for call processing. This could result in the call being terminated. If a malformed line in a SIP message includes information required for the SIP call that the SIP ALG cannot interpret (for example, if an IP address required for SIP NAT is corrupted) the SIP ALG may not be able to continue processing the call and it could be terminated. Discarded messages are counted by SIP ALG static message counters.

Logging and statistics

To record a log message each time the SIP ALG finds a malformed header, enable logging SIP violations in a VoIP profile. In all cases, when the SIP ALG finds an error the FortiGate unit records a malformed header log message that contains information about the error. This happens even if the action is set to pass.

If, because of recording log messages for deep message inspection, the CPU performance is affected by a certain amount, the FortiGate unit records a critical log message about this event and stops writing log messages for deep SIP message inspection.

The following information is recorded in malformed header messages:

- The type of message line in which the error was found.
- The content of the message line in which the error was found (it will be truncated if it makes the log message too long)
- The column or character number in which the error was found (to make it easier to determine what caused the error)

Deep SIP message inspection best practices

Because of the risks imposed by SIP header attacks or incorrect data being allowed and because selecting drop or respond does not require more CPU overhead that pass you would want to set all tests to drop or respond. However, in some cases malformed lines may be less of a threat or risk. For example, the SDP i= does not usually contain information that is parsed by any SIP device so a malformed i= line may not pose a threat.

You can also used the pre-defined VoIP profiles to apply different levels of deep message inspection. The default VoIP profile sets all deep message inspection options to pass and the strict VoIP profile sets all deep message inspection options to discard. From the CLI you can use the `clone` command to copy these pre-defined VoIP profiles and then customize them for your requirements.

Configuring deep SIP message inspection

You configure deep SIP message inspection in a VoIP profile. All deep SIP message inspection options are available only from the CLI.

Enter the following command to configure deep SIP message inspection to discard messages with malformed Request-lines (the first line in a SIP request message):

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set malformed-request-line respond
      end
   end
```

You cannot configure message inspection for the Status-line, which is the first line in a SIP response message.

The following table lists the SIP header lines that the SIP ALG can inspect and the CLI command for configuring the action for each line type. The table also lists the RFC that the header line is defined in.

SIP header lines that the SIP ALG can inspect for syntax errors

SIP Header line	VoIP profile option	RFC
Allow	malformed-header-allow	RFC 3261
Call-ID	malformed-header-call-id	RFC 3261
Contact	malformed-header-contact	RFC 3261
Content-Length	malformed-header-content-length	RFC 3261
Content-Type	malformed-header-content-type	RFC 3261
CSeq	malformed-header-cseq	RFC 3261
Expires	malformed-header-expires	RFC 3261
From	malformed-header-from	RFC 3261
Max-forwards	malformed-header-max-forwards	RFC 3261
P-Asserted-Identity	malformed-header-p-asserted-identity	RFC 3325
RAck	malformed-header-rack	RFC 3262
Record-Route	malformed-header-record-route	RFC 3261
Route	malformed-header-route	RFC 3261
RSeq	malformed-header-rseq	RFC 3262
To	malformed-header-to	RFC 3261
Via	malformed-header-via	RFC 3261

The table below lists the SDP profile lines that the SIP ALG inspects and the CLI command for configuring the action for each line type. SDP profile lines are defined by RFC 4566 and RFC 2327.

SDP profile lines that the SIP ALG can inspect for syntax errors

Attribute	VoIP profile option
a=	malformed-header-sdb-a
b=	malformed-header-sdp-b
c=	malformed-header-sdp-c
i=	malformed-header-sdp-i
k=	malformed-header-sdp-k
m=	malformed-header-sdp-m
o=	malformed-header-sdp-o
r=	malformed-header-sdp-r
s=	malformed-header-sdp-s
t=	malformed-header-sdp-t
v=	malformed-header-sdp-v
z=	malformed-header-sdp-z

Discarding SIP messages with some malformed header and body lines

Enter the following command to configure deep SIP message inspection to discard SIP messages with a malformed Via line, a malformed route line or a malformed m= line but to pass messages with a malformed i= line or a malformed Max-Forwards line

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set malformed-header-via discard
         set malformed-header-route discard
         set malformed-header-sdp-m discard
         set malformed-header-sdp-i pass
         set malformed-header-max-forwards pass
      end
   end
```

Discarding SIP messages with an unknown SIP message type

Enter the following command to discard SIP messages with an unknown SIP message line type as defined in all current SIP RFCs:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set unknown-header discard
      end
   end
```

Discarding SIP messages that exceed a message size

Enter the following command to set the maximum size of a SIP message to 200 bytes. Messages longer than 200 bytes are discarded.

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set max-body-length 200
      end
   end
```

The `max-body-length` option checks the value in the SIP Content-Length header line to determine body length. The Content-Length can be larger than the actual size of a SIP message if the SIP message content is split over more than one packet. SIP message sizes vary widely. The size of a SIP message can also change with the addition of Via and Record-Route headers as the message is transmitted between users and SIP servers.

Discarding SIP messages with lines longer than 500 characters

Enter the following command to set the length of a SIP message line to 500 characters and to block messages that include lines with 500 or more characters:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set max-line-length 500
         set block-long-lines enable
      end
   end
```

Blocking SIP request messages

You may want to block different types of SIP requests:

- to prevent SIP attacks using these messages.
- If your SIP server cannot process some SIP messages because of a temporary issue (for example a bug that crashes or compromises the server when it receives a message of a certain type).
- Your SIP implementation does not use certain message types.

When you enable message blocking for a message type in a VoIP profile, whenever a security policy containing the VoIP profile accepts a SIP message of this type, the SIP ALG silently discards the message and records a log message about the action.

Use the following command to configure a VoIP profile to block SIP CANCEL and Update request messages:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set block-cancel enable
         set block-update enable
```

```
        end
    end
```

SIP uses a variety of text-based messages or requests to communicate information about SIP clients and servers to the various components of the SIP network. Since SIP requests are simple text messages and since the requests or their replies can contain information about network components on either side of the FortiGate unit, it may be a security risk to allow these messages to pass through.

The following table lists all of the VoIP profile SIP request message blocking options. All of these options are disabled by default.

Blocking SIP OPTIONS messages may prevent a redundant configuration from operating correctly. See Supporting geographic redundancy when blocking OPTIONS messages on page 2806 for information about resolving this problem.

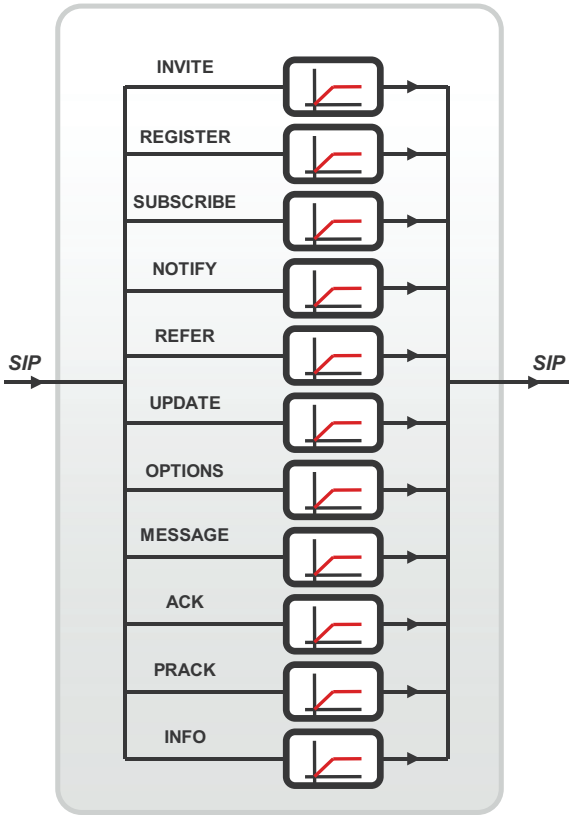
Options for blocking SIP request messages

SIP request message	SIP message blocking CLI Option
ACK	block-ack
BYE	block-bye
Cancel	block-cancel
INFO	block-info
INVITE	block-invite
Message	block-message
Notify	block-notify
Options	block-options
PRACK	block-prack
Publish	block-publish
Refer	block-refer
Register	block-register
Subscribe	block-subscribe
Update	block-update

SIP rate limiting

Configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.

SIP rate limiting



- **SIP message rate limitation**
- **Individually configurable per SIP method**
- **When threshold is hit additional messages with this method will be discarded**
- **Prevents SIP server from getting overloaded by flash crowds or Denial-of-Service attacks.**
- **May block some methods at all** (with extra “block” option)
- **Can be disabled (unlimited rate)**

FortiGate units support rate limiting for the following types of VoIP traffic:

- Session Initiation Protocol (SIP)
- Skinny Call Control Protocol (SCCP) (most versions)
- Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE).

You can use rate limiting of these VoIP protocols to protect the FortiGate unit and your network from SIP and SCCP Denial of Service (DoS) attacks. Rate limiting protects against SIP DoS attacks by limiting the number of SIP REGISTER and INVITE requests that the FortiGate unit receives per second. Rate limiting protects against SCCP DoS attacks by limiting the number of SCCP call setup messages that the FortiGate unit receives per minute.

You configure rate limiting for a message type by specifying a limit for the number of messages that can be received per second. The rate is limited per security policy. When VoIP rate limiting is enabled for a message type, if the a single security policy accepts more messages per second than the configured rate, the extra messages are dropped and log messages are written when the messages are dropped.

Use the following command to configure a VoIP profile to limit the number of INVITE messages accepted by each security policy that the VoIP profile is added to 100 INVITE messages a second:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set invite-rate 100
      end
   end
```

If you are experiencing denial of service attacks from traffic using these VoIP protocols, you can enable VoIP rate limiting and limit the rates for your network. Limit the rates depending on the amount of SIP and SCCP traffic that you expect the FortiGate unit to be handling. You can adjust the settings if some calls are lost or if the amount of SIP or SCCP traffic is affecting FortiGate unit performance.

The table below lists all of the VoIP profile SIP rate limiting options. All of these options are set to 0 so are disabled by default.

Blocking SIP OPTIONS messages may prevent a redundant configuration from operating correctly. See Supporting geographic redundancy when blocking OPTIONS messages on page 2806 for information about resolving this problem.

Options for SIP rate limiting

SIP request message	Rate Limiting CLI Option
ACK	ack-rate
BYE	bye-rate
Cancel	cancel-rate
INFO	info-rate
INVITE	invite-rate
Message	message-rate
Notify	notify-rate
Options	options-rate
PRACK	prack-rate
Publish	publish-rate
Refer	refer-rate
Register	register-rate
Subscribe	subscribe-rate
Update	update-rate

Limiting the number of SIP dialogs accepted by a security policy

In addition to limiting the rates for receiving SIP messages, you can use the following command to limit the number of SIP dialogs (or SIP calls) that the FortiGate unit accepts.

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set max-dialogs 2000
      end
   end
```

This command sets the maximum number of SIP dialogs that can be open for SIP sessions accepted by any security policy that you add the VoIP profile to. The default setting of 0 does not limit the number of dialogs. You can add a limit to control the number of open dialogs and raise and lower it as required. You might want to limit the number of open dialogs for protection against SIP-based attackers opening large numbers of SIP dialogs. Every dialog takes memory and FortiGate CPU resources to process. Limiting the number of dialogs may improve the overall performance of the FortiGate unit. Limiting the number of dialogs will not drop calls in progress but may prevent new calls from connecting.

SIP logging and DLP archiving

You can enable SIP logging and logging of SIP violations, and SIP DLP archiving a VoIP profile. To record SIP log messages you must also enable VoIP event logging in the FortiGate unit event logging configuration.

To view SIP log messages go to **Log&Report > Log Access > Event**.

To view SIP DLP archive messages to go **Log&Report > Archive Access > VoIP**.

Use the following command enable SIP logging, SIP archiving, and logging of SIP violations in a VoIP profile:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set log-call-summary enable
         set log-violations enable
      end
   end
```

Inspecting SIP over SSL/TLS (secure SIP)

Some SIP phones and SIP servers can communicate using SSL or TLS to encrypt the SIP signalling traffic. To allow SIP over SSL/TLS calls to pass through the FortiGate unit, the encrypted signalling traffic has to be unencrypted and inspected. To do this, the FortiGate SIP ALG intercepts and unencrypts and inspects the SIP packets. The packets are then re-encrypted and forwarded to their destination.

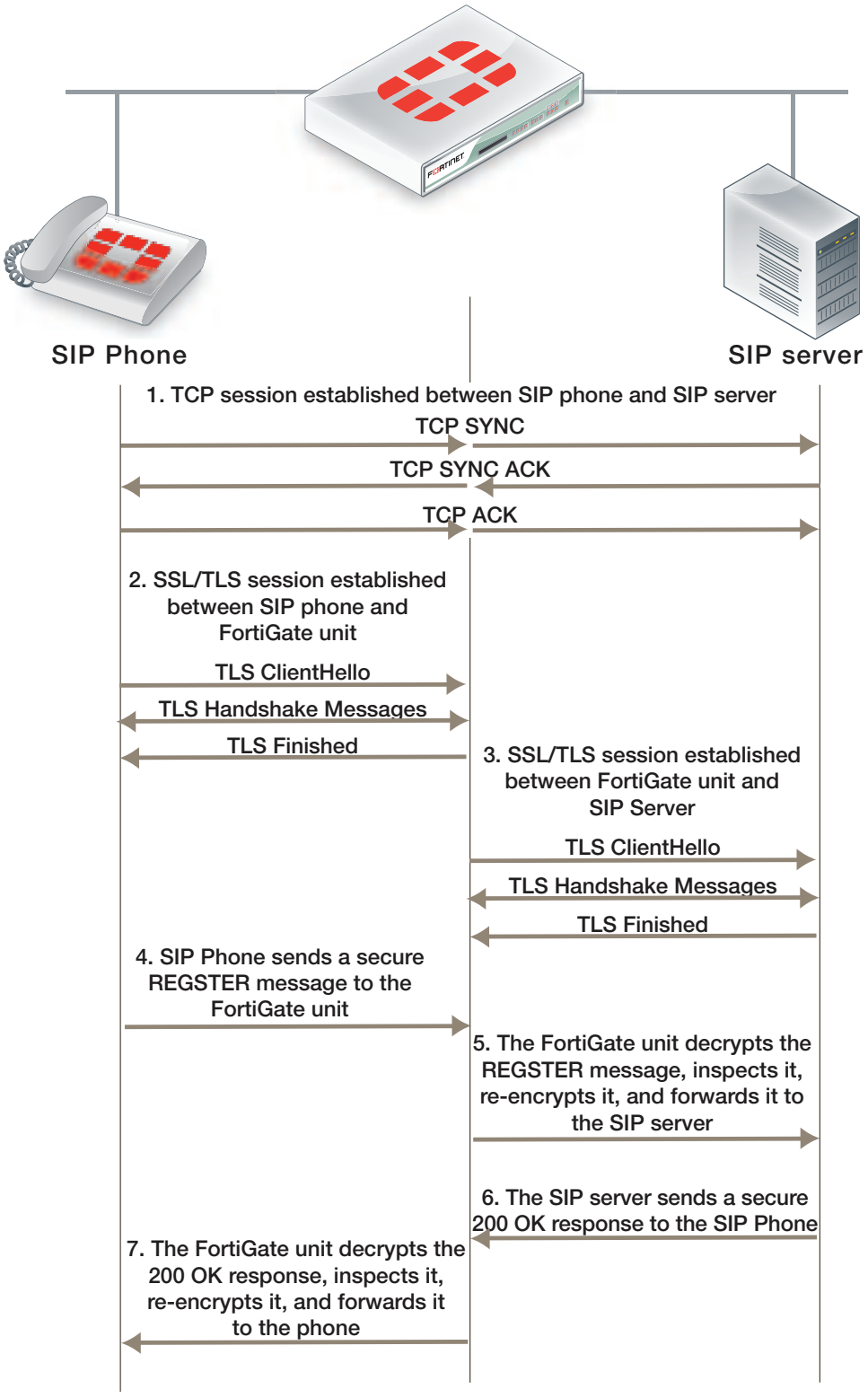
Normally SIP over SSL/TLS uses port 5061. You can use the following command to change the port that the FortiGate listens on for SIP over SSL/TLS sessions to port 5066:

```
config system settings
   set sip-ssl-port 5066
end
```

The SIP ALG supports full mode SSL/TLS only. Traffic between SIP phones and the FortiGate unit and between the FortiGate unit and the SIP server is always encrypted.

You enable SSL/TLS SIP communication by enabling SSL mode in a VoIP profile. You also need to install the SIP server and client certificates on your FortiGate unit and add them to the SSL configuration in the VoIP profile.

SIP over SSL/TLS between a SIP phone and a SIP server



Other than enabling SSL mode and making sure the security policies accept the encrypted traffic, the FortiGate configuration for SSL/TLS SIP is the same as any SIP configuration. SIP over SSL/TLS is supported for all supported SIP configurations.

Adding the SIP server and client certificates

A VoIP profile that supports SSL/TLS SIP requires one certification for the SIP server and one certificate that is used by all of the clients. Use the following steps to add these certificates to the FortiGate unit. Before you start, make sure the client and server certificate files and their key files are accessible from the management computer.

1. Go to **System > Certificates > Local Certificates** and select **Import.**
2. Set **Type** to **Certificate**.
3. Browse to the **Certificate file** and the **Key file** and select **OK**.
4. Enter a password for the certificate and select **OK**.

   The certificate and key are uploaded to the FortiGate unit and added to the **Local Certificates** List.
5. Repeat to upload the other certificate.

The certificates are added to the list of Local Certificates as the filenames you uploaded. You can add comments to make it clear where its from and how it is intended to be used.

Adding SIP over SSL/TLS support to a VoIP profile

Use the following commands to add SIP over SSL/TLS support to the default VoIP profile. The following command enables SSL mode and adds the client and server certificates and passwords, the same ones you entered when you imported the certificates:

```
config voip profile
   edit default
      config sip
         set ssl-mode full
         set ssl-client-certificate "Client_cert"
         set ssl-server-certificate "Server_cert"
         set ssl-auth-client "check-server"
         set ssl-auth-server "check-server-group"
      end
   end
```

Other SSL mode options are also available:

`ssl-send-empty-frags {disable | enable}`	Enable to send empty fragments to avoid CBC IV attacks. Compatible with SSL 3.0 and TLS 1.0 only. Default is `enable`.
`ssl-client-renegotiation {allow | deny | secure}`	Control how the ALG responds when a client attempts to renegotiate the SSL session. You can allow renegotiation or block sessions when the client attempts to renegotiate. You can also select `secure` to reject an SSL connection that does not support RFC 5746 secure renegotiation indication. Default is `allow`.
`ssl-algorithm {high | low | medium}`	Select the relative strength of the algorithms that can be selected. You can select `high`, the default, to allow only AES or 3DES, `medium`, to allow AES, 3DES, or RC4 or `low`, to allow AES, 3DES, RC4, or DES.
`ssl-pfs {allow | deny | regqure}`	Select whether to `allow`, `deny`, or `require` perfect forward secrecy (PFS). Default is `allow`.
`ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1}`	Select the minimum level of SSL support to allow. The default is `ssl-3.0`.
`ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1}`	Select the maximum level of SSL support to allow. The default is `tls-1.1`.

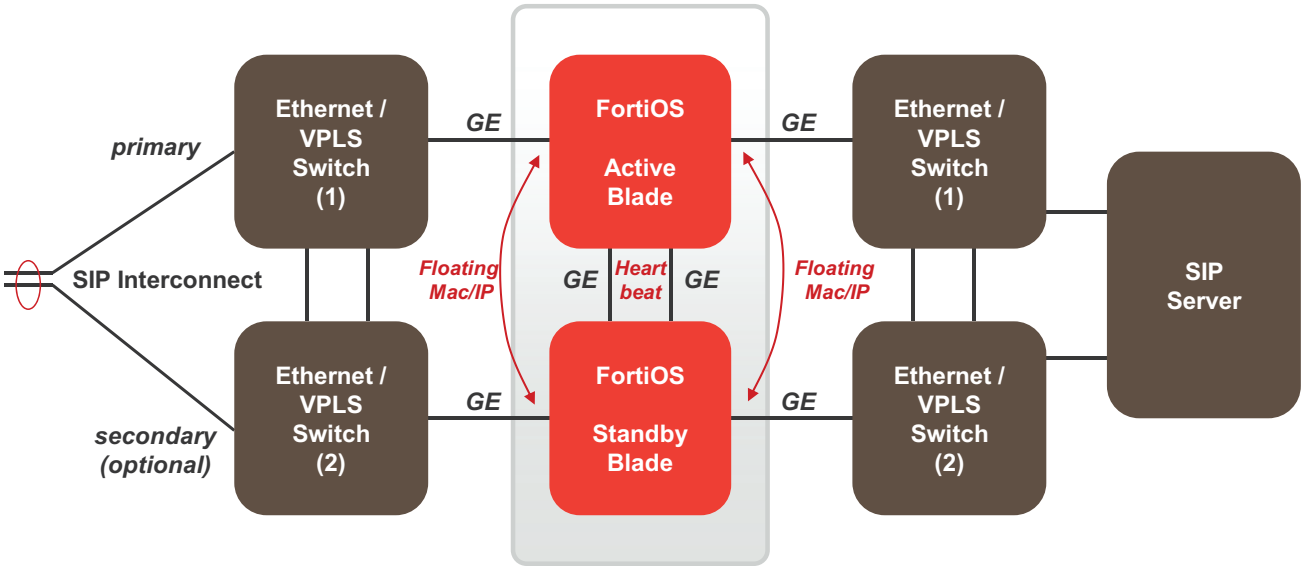
SIP and HA–session failover and geographic redundancy

FortiGate high availability supports SIP session failover (also called stateful failover) for active-passive HA. To support SIP session failover, create a standard HA configuration and select the Enable Session Pick-up option.

SIP session failover replicates SIP states to all cluster units. If an HA failover occurs, all in progress SIP calls (setup complete) and their RTP flows are maintained and the calls will continue after the failover with minimal or no interruption.

SIP calls being set up at the time of a failover may lose signaling messages. In most cases the SIP clients and servers should use message retransmission to complete the call setup after the failover has completed. As a result, SIP users may experience a delay if their calls are being set up when an HA a failover occurs. But in most cases the call setup should be able to continue after the failover.

SIP HA session failover

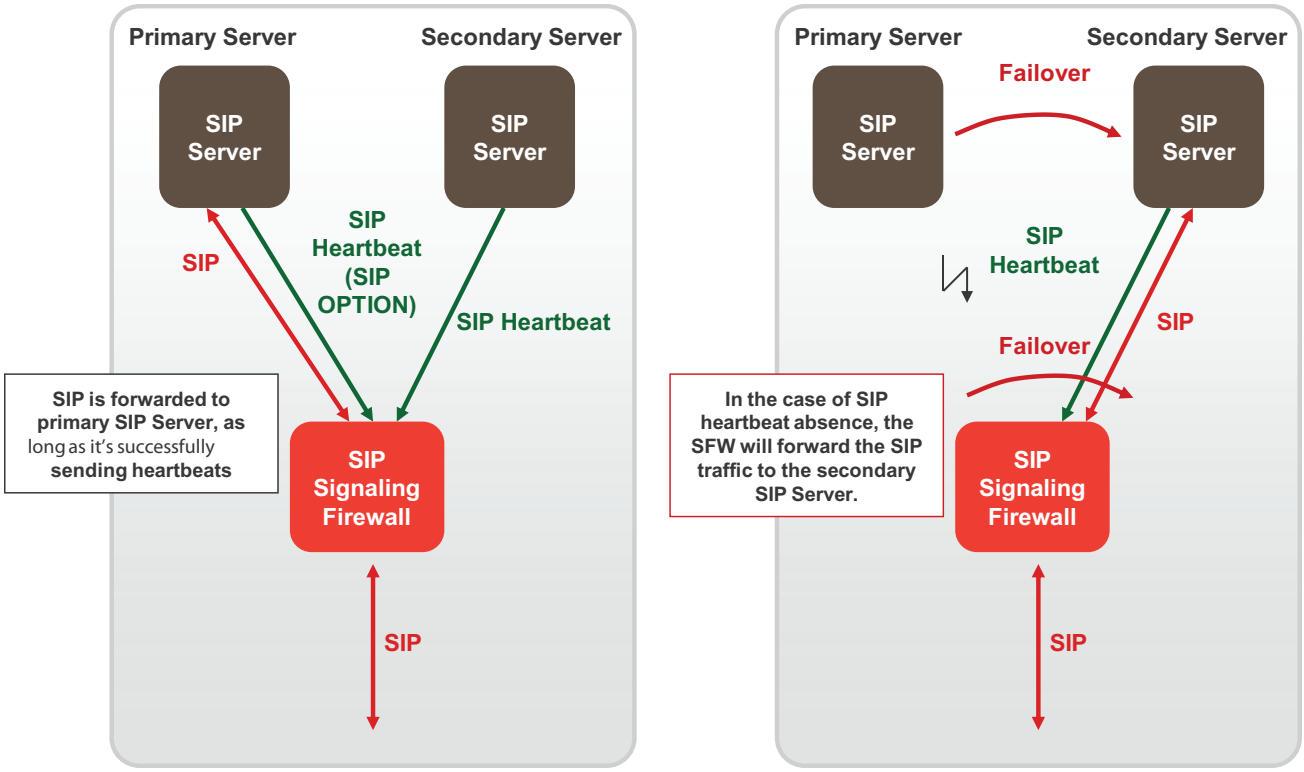


In some cases, failover during call teardown can result in hanging RTP connections which can accumulate over time and use up system memory. If this becomes a problem, you can set a time for the `call-keepalive` SIP VoIP profile setting. The FortiGate will then terminate calls with no activity after the time limit is exceeded. Range is 1 to 10,080 seconds. This options should be used with caution because it results in extra FortiGate CPU overhead and can cause delay/jitter for the VoIP call. Also, the FortiGate unit terminates the call without sending SIP messages to end the call. And if the SIP endpoints send SIP messages to terminate the call they will be blocked by the FortiGate unit if they are sent after the FortiGate unit terminates the call.

SIP geographic redundancy

Maintains a active-standby SIP server configuration, which even supports geographical distribution. If the active SIP server fails (missing SIP heartbeat messages or SIP traffic) FortiOS will redirect the SIP traffic to a secondary SIP server. SIP geographic redundancy

Geographic redundancy



Supporting geographic redundancy when blocking OPTIONS messages

For some geographic redundant SIP configurations, the SIP servers may use SIP OPTIONS messages as heartbeats to notify the FortiGate unit that they are still operating (or alive). This is a kind of passive SIP monitoring mechanism where the FortiGate unit isn't actively monitoring the SIP servers and instead the FortiGate unit passively receives and analyzes OPTIONS messages from the SIP servers.

If FortiGate units block SIP OPTIONS messages because `block-options` is enabled, the configuration may fail to operate correctly because the OPTIONS messages are blocked by one or more FortiGate units.

However, you can work around this problem by enabling the `block-geo-red-options` application control list option. This option causes the FortiGate unit to refresh the local SIP server status when it receives an OPTIONS message before dropping the message. The end result is the heartbeat signals between geographically redundant SIP servers are maintained but OPTIONS messages do not pass through the FortiGate unit.

Use the following command to block OPTIONS messages while still supporting geographic redundancy:

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set block-options disable
         set block-geo-red-options enable
      end
end
```

The `block-options` option setting overrides the `block-geo-red-options` option. If `block-options` is enabled the FortiGate unit only blocks SIP OPTIONS messages and does not refresh local SIP server status.

Support for RFC 2543-compliant branch parameters

RFC 3261 is the most recent SIP RFC, it obsoletes RFC 2543. However, some SIP implementations may use RFC 2543-compliant SIP calls.

The `rfc2543-branch` VoIP profile option allows the FortiGate unit to support SIP calls that include an RFC 2543-compliant branch parameter in the SIP Via header. This option also allows FortiGate units to support SIP calls that include Via headers that are missing the branch parameter.

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set rfc2543-branch enable
      end
   end
```

SIP and IPS

You can enable IPS in security policies that also accept SIP sessions to protect the SIP traffic from SIP-based attacks. If you enable IPS in this way then by default the pinholes that the SIP ALG creates to allow RTP and RTCP to flow through the firewall will also have IPS enabled.

This inheritance of the IPS setting can cause performance problems if the RTP traffic volume is high since IPS checking may reduce performance in some cases. Also if you are using network processor (NP) interfaces to accelerate VoIP performance, when IPS is enabled for the pinhole traffic is diverted to the IPS and as a result is not accelerated by the network processors.

You can use the following CLI command to disable IPS for the RTP pinhole traffic.

```
config voip profile
   edit VoIP_Pro_Name
      config sip
         set ips-rtp disable
      end
   end
```

SIP debugging

SIP debug log format

Assuming that `diagnose debug console timestamp` is enabled then the following shows the debug that is generated for an INVITE if `diag debug appl sip -1` is enabled:

```
2010-01-04 21:39:59 sip port 26 locate session for 192.168.2.134:5061 ->
172.16.67.192:5060
2010-01-04 21:39:59 sip sess 0x979df38 found for 192.168.2.134:5061 ->
172.16.67.192:5060
2010-01-04 21:39:59 sip port 26 192.168.2.134:5061 -> 172.16.67.192:5060
2010-01-04 21:39:59 sip port 26 read [(0,515)
```

```
00d0a46726f6d3a2073697070203c7369703a73697070403132372e302e312e313a353036313e3b7461673d36383237534950705
4616730303632300d0a546f3a20737574203c7369703a736572766963654031393322e3136382e322e3130303a353036303e0d0a4
3616c6c2d49443a203632302d36383237403132372e302e312e310d0a435365713a203120494e564954450d0a436f6e746163743
a207369703a73697070403132372e302e312e313a353036310d0a4d61782d466f7277617264733a2037300d0a5375626a6563743
a20506572666f726d616e636520546573740d0a436f6e74656e742d547970653a206170706c69636174696f6e2f7364700d0a436
f6e74656e742d4c656e6774683a20203132390d0a0d0a763d300d0a6f3d7573657231203533363535373635203233353333638373
6333720494e20495034203132372e302e312e310d0a733d2d0d0a633d494e20495034203132372e302e312e310d0a743d3020300
d0a6d3d617564696f203630303120525450 2f41565020300d0a613d7274706d61703a3020504434d552f383030300d0a)(INVITE
sip:service@192.168.2.100:5060 SIP/2.0..Via: SIP/2.0/UDP
127.0.1.1:5061;branch=z9hG4bK-6827-620-0..From: sipp
%lt;sip:sipp@127.0.1.1:5061>;tag=6827SIPpTag00620..To: sut
%lt;sip:service@192.168.2.100:5060>..Call-ID: 620-6827@127.0.1.1..CSeq: 1
INVITE..Contact: sip:sipp@127.0.1.1:5061..Max-Forwards: 70..Subject: Performance
Test..Content-Type: application/sdp..Content-Length: 129....v=0..o=user1 53655765
2353687637 IN IP4 127.0.1.1..s=-..c=IN IP4 127.0.1.1..t=0 0..m=audio 6001 RTP/AVP
0..a=rtpmap:0 PCMU/8000..)]
2010-01-04 21:39:59 sip port 26 len 515
2010-01-04 21:39:59 sip port 26 INVITE '192.168.2.100:5060' addr 192.168.2.100:5060
2010-01-04 21:39:59 sip port 26 CSeq: 1 INVITE
2010-01-04 21:39:59 sip port 26 Via: UDP 127.0.1.1:5061 len 14 received 0 rport 0 0 branch 'z9hG4bK-
6827-620-0'
2010-01-04 21:39:59 sip port 26 From: 'sipp ;tag=6827SIPpTag00620' URI 'sip:sipp@127.0.1.1:5061' tag
'6827SIPpTag00620'
2010-01-04 21:39:59 sip port 26 To: 'sut ' URI 'sip:service@192.168.2.100:5060' tag ''
2010-01-04 21:39:59 sip port 26 Call-ID: '620-6827@127.0.1.1'
2010-01-04 21:39:59 sip port 26 Contact: '127.0.1.1:5061' addr 127.0.1.1:5061 expires 0
2010-01-04 21:39:59 sip port 26 Content-Length: 129 len 3
2010-01-04 21:39:59 sip port 26 sdp o=127.0.1.1 len=9
2010-01-04 21:39:59 sip port 26 sdp c=127.0.1.1 len=9
2010-01-04 21:39:59 sip port 26 sdp m=6001 len=4
2010-01-04 21:39:59 sip port 26 find call 0 '620-6827@127.0.1.1'
2010-01-04 21:39:59 sip port 26 not found
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 open (collision (nil))
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 open txn 0x979f7f8 INVITE dir 0
2010-01-04 21:39:59 sip port 26 sdp i: 127.0.1.1:6001
2010-01-04 21:39:59 sip port 26 policy id 1 is_client_vs_policy 1 policy_dir_rev 0
2010-01-04 21:39:59 sip port 26 policy 1 not RTP policy
2010-01-04 21:39:59 sip port 26 learn sdp from stream address
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 sdp 172.16.67.198:43722
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 txn 0x979f7f8 127.0.1.1:5061 find new address and port
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 txn 0x979f7f8 127.0.1.1:5061 find new address and port
2010-01-04 21:39:59 sip port 26 call 0x97a47c0 txn 0x979f7f8 127.0.1.1:5061 find new address and port
2010-01-04 21:39:59 sip port 30 write 192.168.2.134:5061 -> 172.16.67.192:5060 (13,539)
2010-01-04 21:39:59 sip port 30 write [(13,539)
(494e56495445207369703a736572766963654031373 22e31362e36372e3139323a353036302 05349502f322e300d0a5669613a2
05349502f322e302f554450203137322e31362e36372e3139383a35323036353b6272616e63683d7a39684734624b2d363832372
d3632302d300d0a46726f6d3a2073697070203c7369703a73697070403137322e31362e36372e3139383a34333732343e3b74616
73d3638323753495070546167303036323 00d0a546f3a20737574203c7369703a736572766963654031373 22e31362e36372e313
9323a353036303e0d0a43616c6c2d49443a203632302d36383237403132372e302e312e310d0a435365713a203120494e5649544
50d0a436f6e746163743a207369703a73697070403137322e31362e36372e3139383a343337323 50d0a4d61782d466f727761726
4733a2037300d0a5375626a6563743a20506572666f726d616e636520546573740d0a436f6e74656e742d547970653a206170706
c69636174696f6e2f7364700d0a436f6e74656e742d4c656e6774683a20203133380d0a0d0a763d300d0a6f3d757365723120353
3363535373635203233353336383736333720494e20495034203137322e31362e36372e3139380d0a733d2d0d0a633d494e20495
034203137322e31362e36372e3139380d0a743d3020300d0a6d3d617564696f203433373232205254502f41565020300d0a613d7
274706d61703a302050434d552f383030300d0a)(INVITE sip:service@172.16.67.192:5060 SIP/2.0..Via: SIP/2.0/UDP
172.16.67.198:52065;branch=z9hG4bK-6827-620-0..From: sipp ;tag=6827SIPpTag00620..To: sut ..Call-ID: 620-
6827@127.0.1.1..CSeq: 1 INVITE..Contact: sip:sipp@172.16.67.198:43725..Max-Forwards: 70..Subject:
Performance Test..Content-Type: application/sdp..Content-Length: 138....v=0..o=user1 53655765 2353687637
IN IP4 172.16.67.198..s=-..c=IN IP4 172.16.67.198..t=0 0..m=audio 43722 RTP/AVP 0..a=rtpmap:0
PCMU/8000..)]
```

SIP-proxy filter per VDOM

You can use the `diagnose sys sip-proxy xxx` command in a VDOM to get info about how SIP is operating in each VDOM.

SIP-proxy filter command

Use the `diagnose sys sip-proxy filter` to filter diagnose information for the SIP ALG. The following filters are available:

```
diag sys sip-proxy filter vd
diag sys sip-proxy filter dst-addr4
diag sys sip-proxy filter dst-addr6
diag sys sip-proxy filter dst-port
diag sys sip-proxy filter identity-policy
diag sys sip-proxy filter negate
diag sys sip-proxy filter policy
diag sys sip-proxy filter policy-type
diag sys sip-proxy filter profile-group
diag sys sip-proxy filter src-addr4
diag sys sip-proxy filter src-addr6
diag sys sip-proxy filter src-port
diag sys sip-proxy filter vd
diag sys sip-proxy filter voip-profile
```

You can clear, view and negate/invert the sense of a filter using these commands:

```
diag sys sip-proxy filter clear
diag sys sip-proxy filter list
diag sys sip-proxy filter negate
```

SIP debug log filtering

You can filter by VDOM/IP/PORT and by policy and VoIP profile. The filtering can be controlled by:

```
diagnose sys sip-proxy log-filter
```

The list of filters is:

```
diag sys sip-proxy log-filter vd
diag sys sip-proxy log-filter dst-addr4
diag sys sip-proxy log-filter dst-addr6
diag sys sip-proxy log-filter dst-port
diag sys sip-proxy log-filter identity-policy
diag sys sip-proxy log-filter policy
diag sys sip-proxy log-filter policy-type
diag sys sip-proxy log-filter profile-group
diag sys sip-proxy log-filter src-addr4
diag sys sip-proxy log-filter src-addr6
diag sys sip-proxy log-filter src-port
diag sys sip-proxy log-filter vd
diag sys sip-proxy log-filter voip-profile
```

You can clear, view and negate/invert the sense of a filter using these commands:

```
diag sys sip-proxy log-filter clear
diag sys sip-proxy log-filter list
diag sys sip-proxy log-filter negate
```

SIP debug setting

Control of the SIP debug output is governed by the following command

```
diagnose debug application sip <debug_level_int>
```

Where the <debug_level_int> is a bitmask and the individual values determine whether the listed items are logged or not. The <debug_level_int> can be:

1	Configuration changes, mainly addition/deletion/modification of virtual domains.
2	TCP connection accepts or connects, redirect creation.
4	Create or delete a session.
16	Any IO read or write.
32	An ASCII dump of all data read or written.
64	Include HEX dump in the above output.
128	Any activity related to the use of the FortiCarrier dynamic profile feature to determine the correct profile-group to use.
256	Log summary of interesting fields in a SIP call.
1024	Any activity related to SIP geo-redundancy.
2048	Any activity related to HA syncing of SIP calls.

Display SIP rate-limit data

You can use the `diagnose sys sip-proxy meters` command to display SIP rate limiting data.

For the following command output `rate 1` shows that the current (over last second) measured rate for INVITE/ACK and BYTE was 1 per second, the `peak 1` shows that the peak rate recorded is 1 per second, the `max 0` shows that there is no maximum limit set, the `count 18` indicates that 18 messages were received and `drop 0` indicates that none were dropped due to being over the limit.

```
diag sys sip-proxy meters
sip
sip vd: 0
sip policy: 1
sip identity-policy: 0
sip policy-type: IPv4
sip profile-group:
sip dialogs: 18
sip dialog-limit: 0
sip UNKNOWN: rate 0 peak 0 max 0 count 0 drop 0
sip ACK: rate 1 peak 1 max 0 count 18 drop 0
sip BYE: rate 1 peak 1 max 0 count 18 drop 0
sip CANCEL: rate 0 peak 0 max 0 count 0 drop 0
sip INFO: rate 0 peak 0 max 0 count 0 drop 0
sip INVITE: rate 1 peak 1 max 0 count 18 drop 0
sip MESSAGE: rate 0 peak 0 max 0 count 0 drop 0
sip NOTIFY: rate 0 peak 0 max 0 count 0 drop 0
sip OPTIONS: rate 0 peak 0 max 0 count 0 drop 0
sip PRACK: rate 0 peak 0 max 0 count 0 drop 0
sip PUBLISH: rate 0 peak 0 max 0 count 0 drop 0
sip REFER: rate 0 peak 0 max 0 count 0 drop 0
```

```
sip REGISTER: rate 0 peak 0 max 0 count 0 drop 0
sip SUBSCRIBE: rate 0 peak 0 max 0 count 0 drop 0
sip UPDATE: rate 0 peak 0 max 0 count 0 drop 0
sip PING: rate 0 peak 0 max 0 count 0 drop 0
sip YAHOOREF: rate 0 peak 0 max 0 count 0 drop 0
```

Chapter 30 - WAN Optimization, Web Cache, Explicit Proxy, and WCCP

You configure all of these features by creating security policies and adding WAN Optimization, web caching, and proxying to them. These same security policies can also include security profiles that apply UTM and NGFW features to WAN Optimization, web caching, and explicit proxy traffic.

The FortiOS Handbook chapter contains the following sections:

- Example network topologies provides an overview of FortiGate WAN optimization best practices and technologies and some of the concepts and rules for using them. We recommend that you begin with this chapter before attempting to configure your FortiGate unit to use WAN optimization.
- Configuring WAN optimization provides basic configuration for WAN optimization rules, including adding rules, organizing rules in the rule list and using WAN optimization addresses. This chapter also explains how WAN optimization accepts sessions, as well as how and when you can apply security profiles to WAN optimization traffic.
- Peers and authentication groups describes how to use WAN optimization peers and authentication groups to control access to WAN optimization tunnels.
- Configuration examples describes basic active-passive and peer-to-peer WAN optimization configuration examples. This chapter is a good place to start learning how to put an actual WAN optimization network together.
- Web caching and SSL offloading describes how web caching works to cache HTTP and HTTPS, how to use SSL offloading to improved performance of HTTPS websites, and includes web caching configuration examples.
- FortiClient WAN optimization describes how FortiGate and FortiClient WAN optimization work together and includes an example configuration.
- The FortiGate explicit web proxy describes how to configure the FortiGate explicit web proxy, how users connect to the explicit web proxy, and how to add web caching to the explicit web proxy.
- The FortiGate explicit FTP proxy describes how to configure the FortiGate explicit FTP proxy and how users connect to the explicit FTP proxy.
- FortiGate WCCP describes FortiGate WCCP and how to configure WCCP and the WCCP client.
- Diagnose commands describes get and diagnose commands available for troubleshooting WAN optimization, web cache, and WCCP.

Example network topologies

FortiGate WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, web caching, SSL offloading, and secure tunneling. Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiGate units to reduce the amount of data transmitted across the WAN. Web caching stores web pages on FortiGate units to reduce latency and delays between the WAN and web servers. SSL offloading offloads SSL decryption and encryption from web servers onto FortiGate SSL acceleration hardware. Secure tunneling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP and HTTPS traffic, you can also apply protocol optimization and web caching.

You can configure a FortiGate unit to be an explicit web proxy server for both IPv4 and IPv6 traffic and an explicit FTP proxy server. Users on your internal network can browse the Internet through the explicit web proxy server or connect to FTP servers through the explicit FTP proxy server. You can also configure these proxies to protect access to web or FTP servers behind the FortiGate unit using a reverse proxy configuration.

Web caching can be applied to any HTTP or HTTPS traffic, this includes normal traffic accepted by a security policy, explicit web proxy traffic, and WAN optimization traffic.

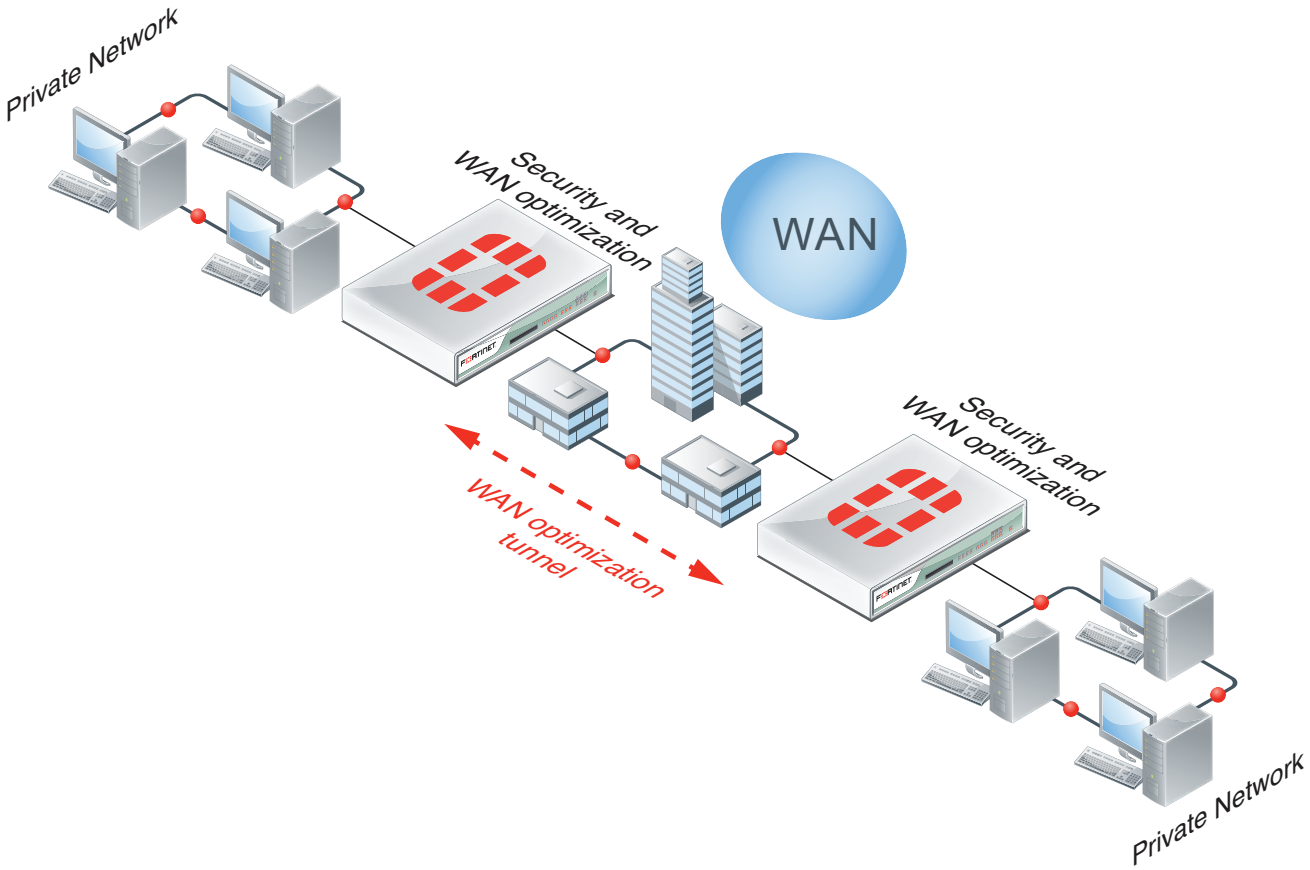
You can also configure a FortiGate unit to operate as a Web Cache Communication Protocol (WCCP) client or server. WCCP provides the ability to offload web caching to one or more redundant web caching servers.

FortiGate units can also apply security profiles to traffic as part of a WAN optimization, explicit web proxy, explicit FTP proxy, web cache and WCCP configuration. Security policies that include any of these options can also include settings to apply all forms of security profiles supported by your FortiGate unit.

Basic WAN optimization topology

The basic FortiGate WAN optimization topology consists of two FortiGate units operating as WAN optimization peers intercepting and optimizing traffic crossing the WAN between the private networks.

Security device and WAN optimization topology



FortiGate units can be deployed as security devices that protect private networks connected to the WAN and also perform WAN optimization. In this configuration, the FortiGate units are configured as typical security devices for the private networks and are also configured for WAN optimization. The WAN optimization configuration intercepts traffic to be optimized as it passes through the FortiGate unit and uses a WAN optimization tunnel with another FortiGate unit to optimize the traffic that crosses the WAN.

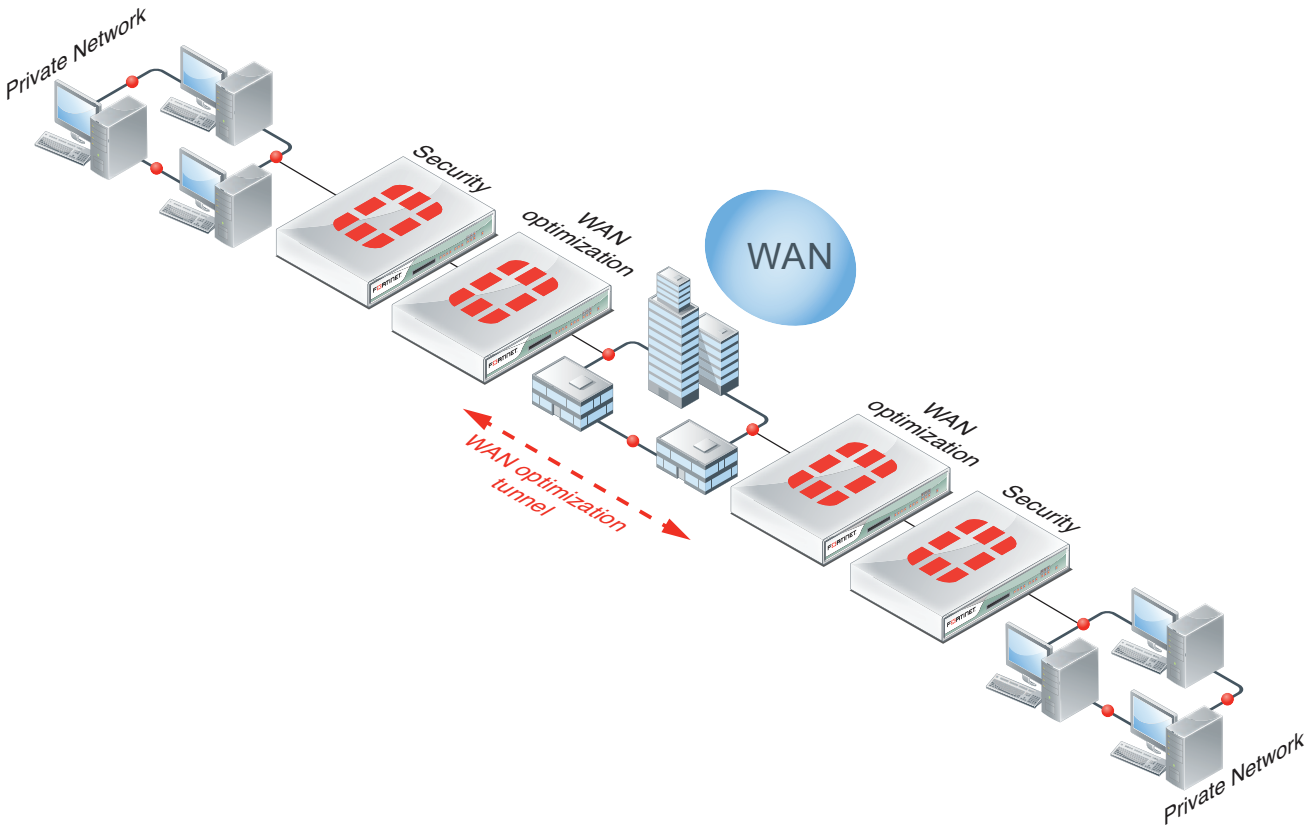
You can also deploy WAN optimization on single-purpose FortiGate units that only perform WAN optimization. In the out of path WAN optimization topology shown below, FortiGate units are located on the WAN outside of the private networks. You can also install the WAN optimization FortiGate units behind the security devices on the private networks.

The WAN optimization configuration is the same for FortiGate units deployed as security devices and for single-purpose WAN optimization FortiGate units. The only differences would result from the different network topologies.

Out-of-path WAN Optimization topology

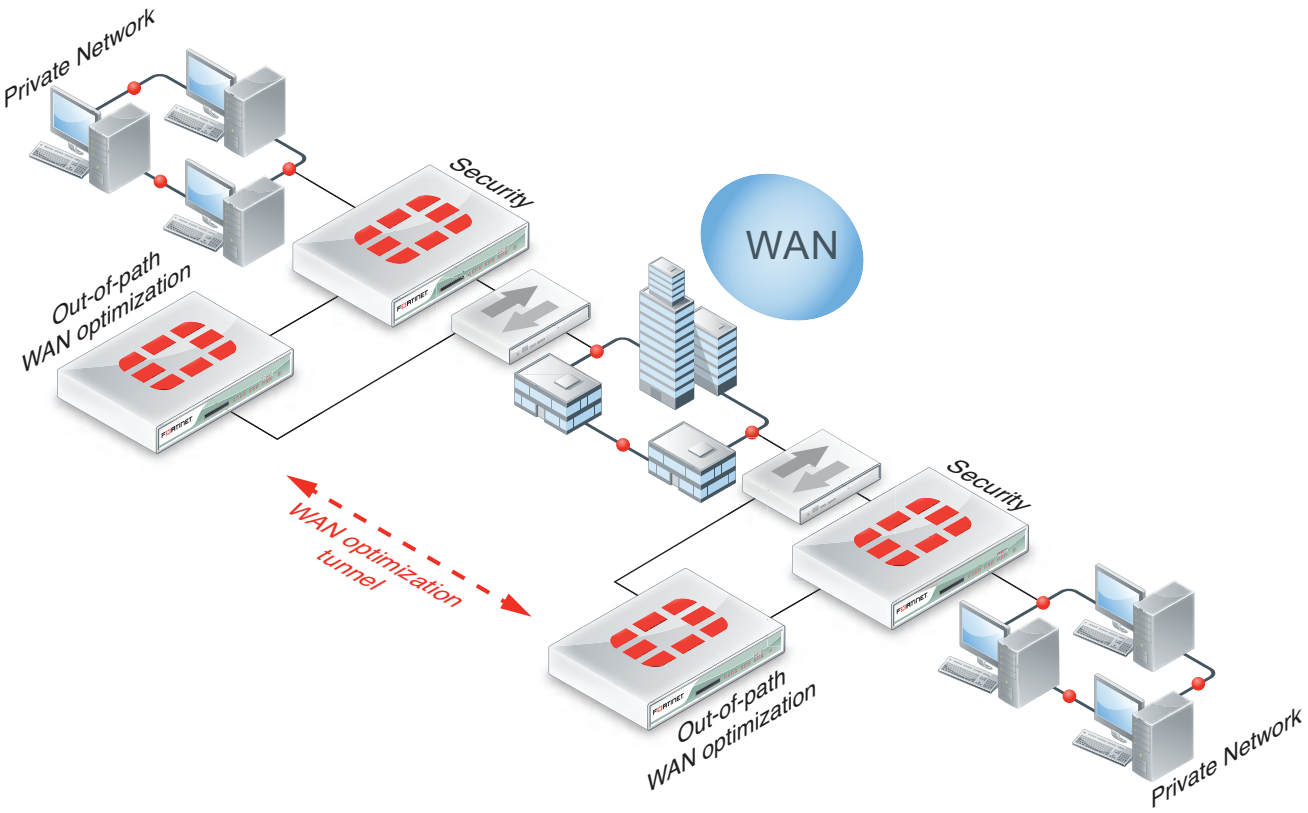
In an out-of-path topology, one or both of the FortiGate units configured for WAN optimization are not directly in the main data path. Instead, the out-of-path FortiGate unit is connected to a device on the data path, and the device is configured to redirect sessions to be optimized to the out-of-path FortiGate unit.

Single-purpose WAN optimization topology



The following out-of-path FortiGate units are configured for WAN optimization and connected directly to FortiGate units in the data path. The FortiGate units in the data path use a method such as policy routing to redirect traffic to be optimized to the out-of-path FortiGate units. The out-of-path FortiGate units establish a WAN optimization tunnel between each other and optimize the redirected traffic.

Out-of-path WAN optimization



One of the benefits of out-of-path WAN optimization is that out-of-path FortiGate units only perform WAN optimization and do not have to process other traffic. An in-path FortiGate unit configured for WAN optimization also has to process other non-optimized traffic on the data path.

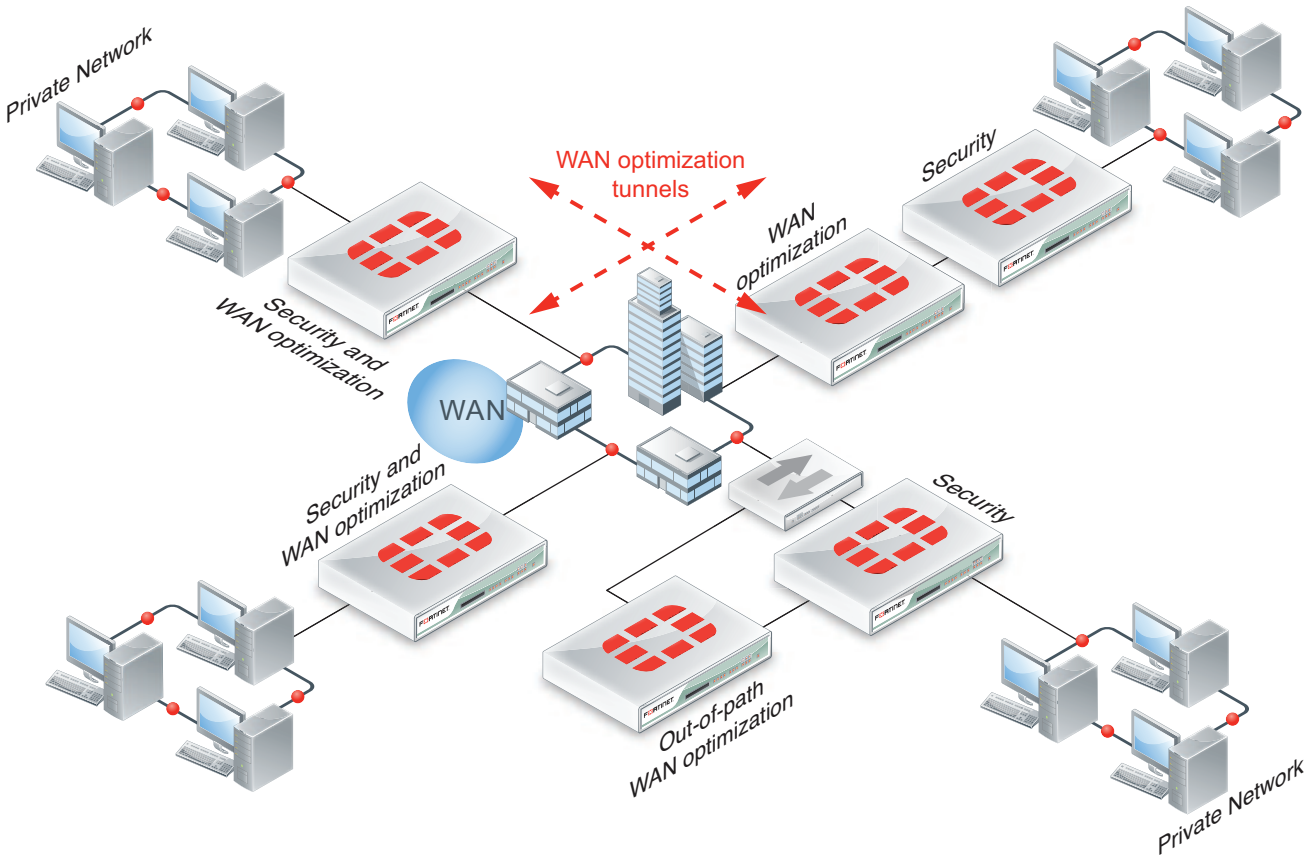
The out-of-path FortiGate units can operate in NAT/Route or Transparent mode.

Other out-of-path topologies are also possible. For example, you can install the out-of-path FortiGate units on the private networks instead of on the WAN. Also, the out-of-path FortiGate units can have one connection to the network instead of two. In a one-arm configuration such as this, security policies and routing have to be configured to send the WAN optimization tunnel out the same interface as the one that received the traffic.

Topology for multiple networks

As shown in below, you can create multiple WAN optimization configurations between many private networks. Whenever WAN optimization occurs, it is always between two FortiGate units, but you can configure any FortiGate unit to perform WAN optimization with any of the other FortiGate units that are part of your WAN.

WAN optimization among multiple networks

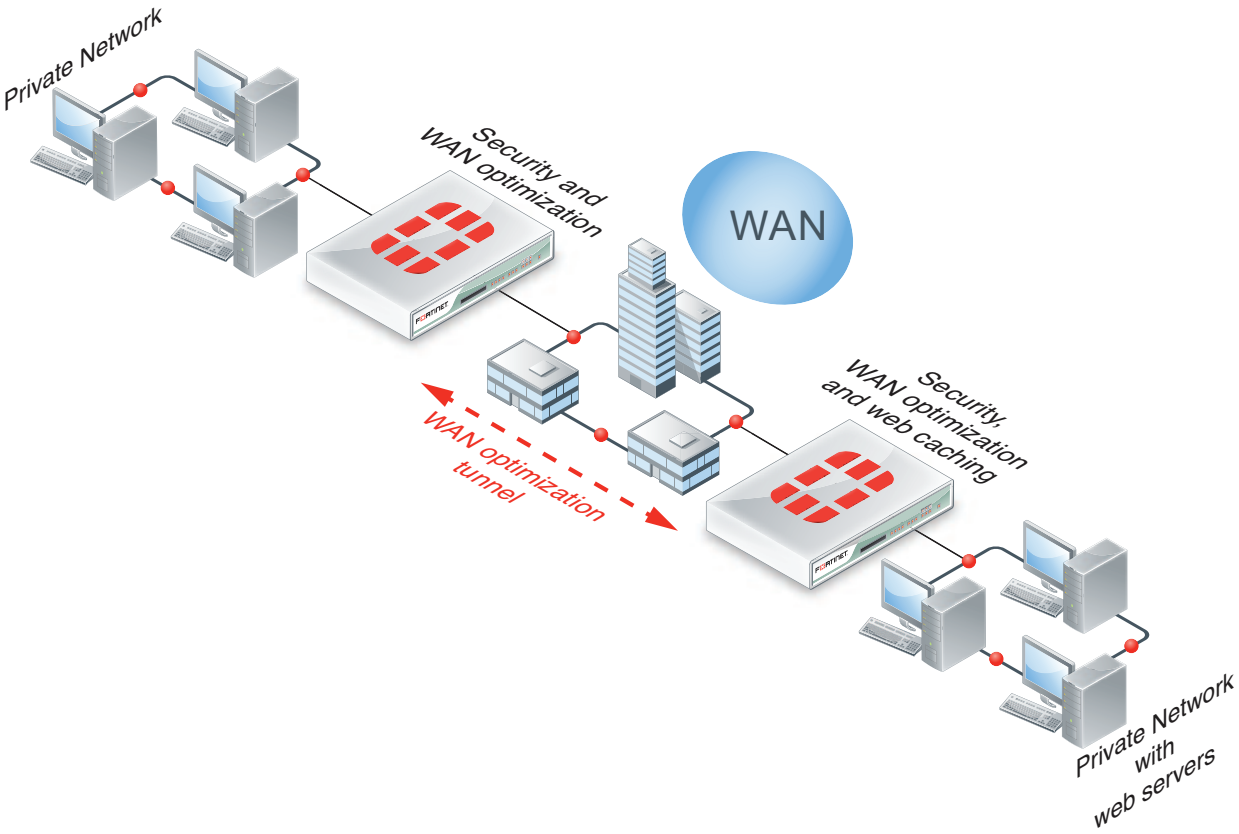


You can also configure WAN optimization between FortiGate units with different roles on the WAN. FortiGate units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiGate units just configured for WAN optimization.

WAN optimization with web caching

You can add web caching to a WAN optimization topology when users on a private network communicate with web servers located across the WAN on another private network.

WAN optimization with web caching topology

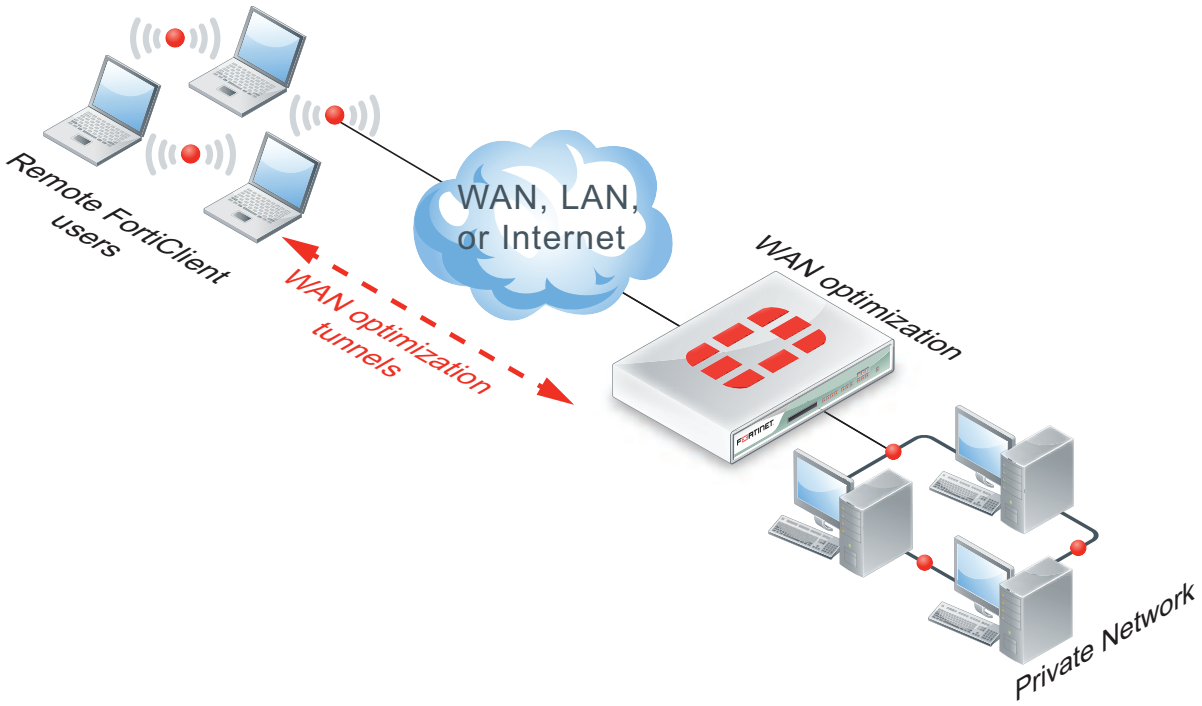


The topology above is the same as that shown in Basic WAN optimization topology on page 2813 with the addition of web caching to the FortiGate unit in front of the private network that includes the web servers. You can also add web caching to the FortiGate unit that is protecting the private network. In a similar way, you can add web caching to any WAN Optimization topology.

WAN optimization and web caching with FortiClient peers

FortiClient WAN optimization works with FortiGate WAN optimization to accelerate remote user access to the private networks behind FortiGate units. The FortiClient application requires a simple WAN optimization configuration to automatically detect if WAN optimization is enabled on the FortiGate unit. Once WAN optimization is enabled, the FortiClient application transparently makes use of the WAN optimization and web caching features available.

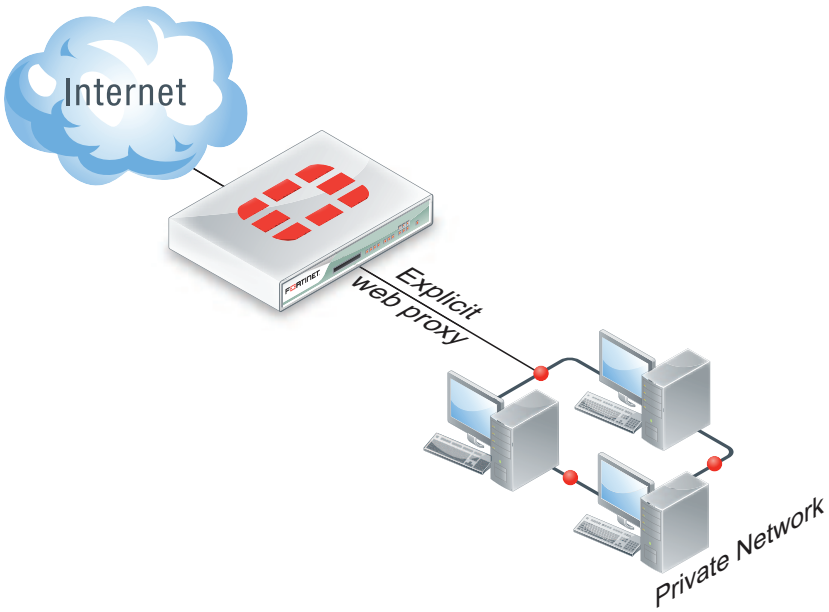
FortiClient WAN optimization topology



Explicit Web proxy topologies

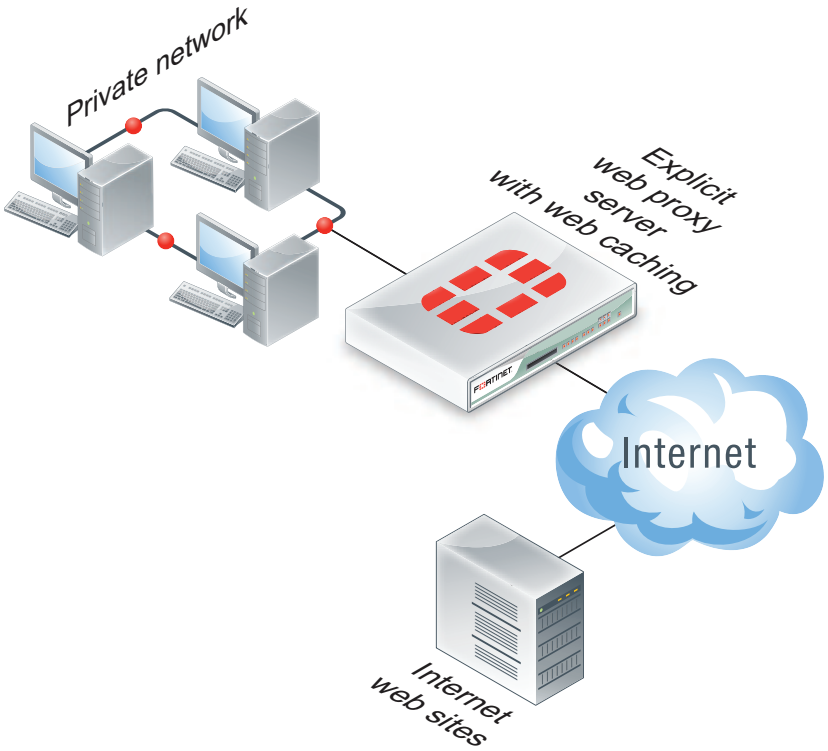
You can configure a FortiGate unit to be an explicit web proxy server for Internet web browsing of IPv4 and IPv6 web traffic. To use the explicit web proxy, users must add the IP address of the FortiGate interface configured for the explicit web proxy to their web browser proxy configuration.

Explicit web proxy topology



If the FortiGate unit supports web caching, you can also add web caching to the security policy that accepts explicit web proxy sessions The FortiGate unit then caches Internet web pages on a hard disk to improve web browsing performance.

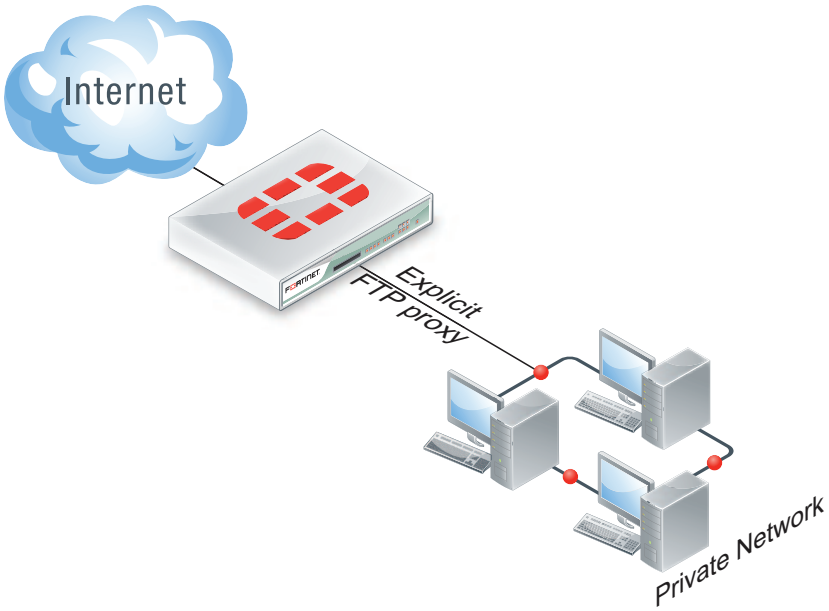
Explicit web proxy with web caching topology



Explicit FTP proxy topologies

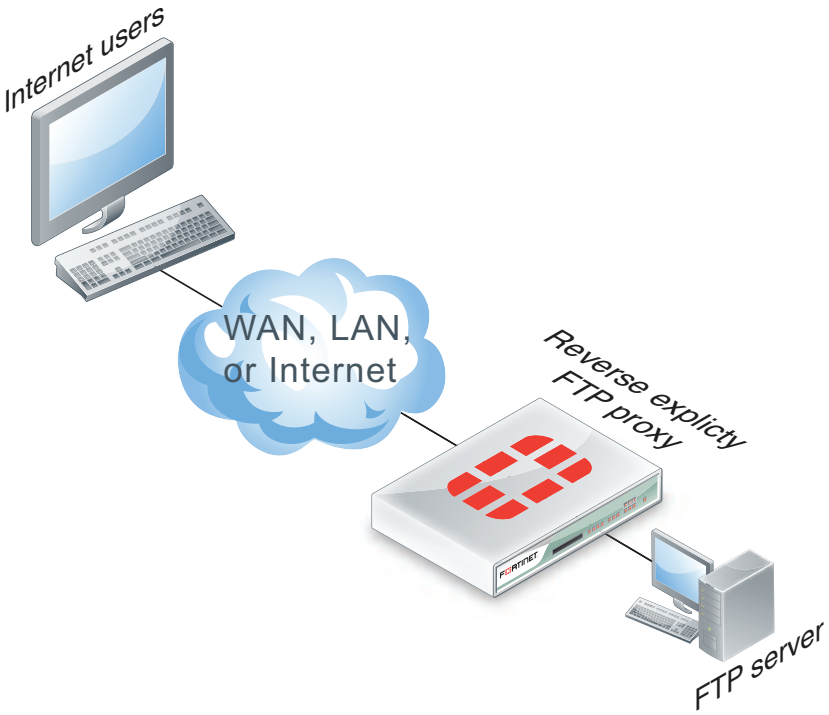
You can configure a FortiGate unit to be an explicit FTP proxy server for FTP users. To use the explicit web proxy, FTP users must connect to and authenticate with the explicit FTP proxy before connecting to an FTP server.

Explicit FTP proxy topology



You can also configure reverse explicit FTP proxy. In this configuration, users on the Internet connect to the explicit web proxy before connecting to an FTP server installed behind a FortiGate unit.

Reverse explicit FTP proxy topology

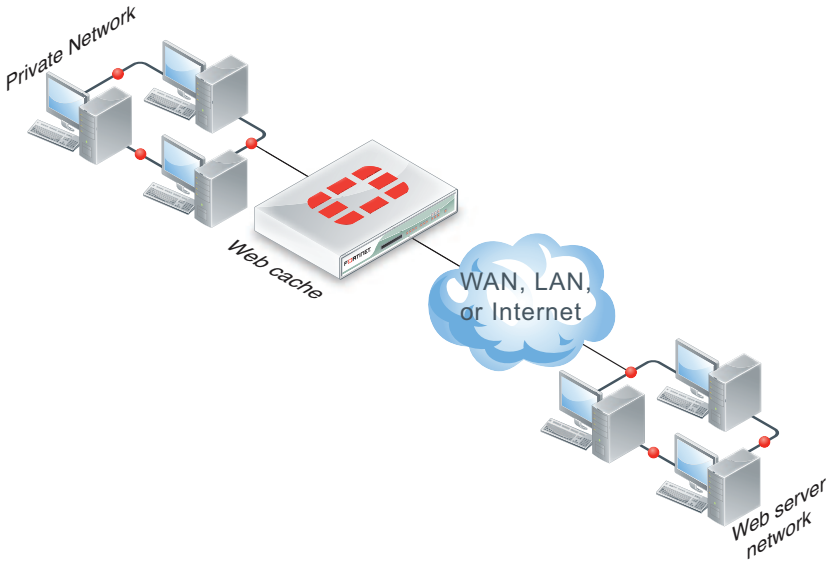


Web caching topologies

FortiGate web caching can be added to any security policy and any HTTP or HTTPS traffic accepted by that security policy can be cached on the FortiGate unit hard disk. This includes WAN optimization and explicit web proxy traffic. The network topologies for these scenarios are very similar. They involved a FortiGate unit installed between users and web servers with web caching enabled.

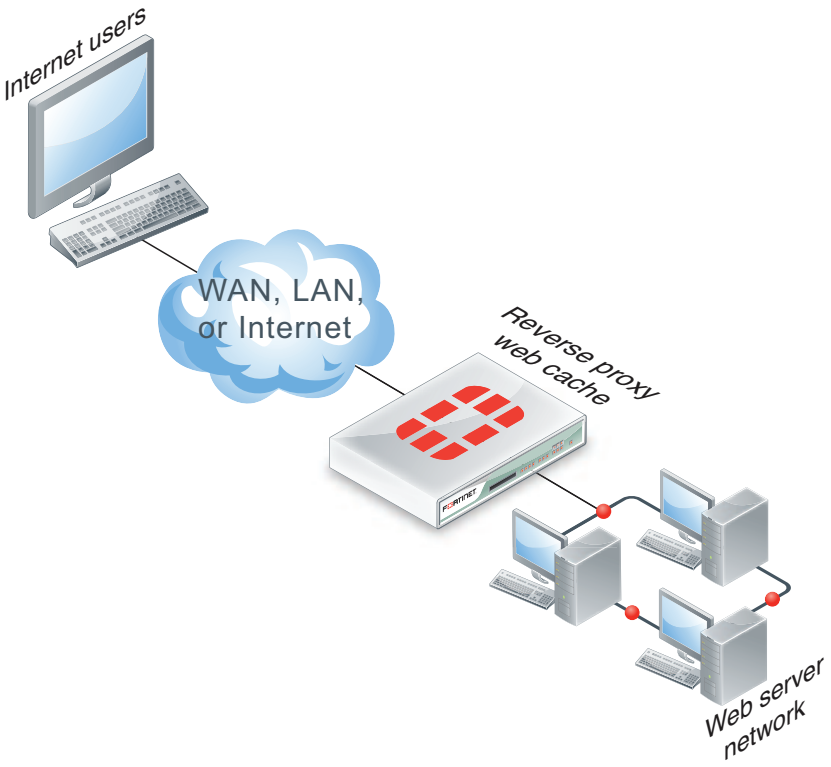
A typical web-caching topology includes one FortiGate unit that acts as a web cache server. Web caching is enabled in a security policy and the FortiGate unit intercepts web page requests accepted by the security policy, requests web pages from the web servers, caches the web page contents, and returns the web page contents to the users. When the FortiGate unit intercepts subsequent requests for cached web pages, the FortiGate unit contacts the destination web server just to check for changes.

Web caching topology



You can also configure reverse proxy web-caching. In this configuration, users on the Internet browse to a web server installed behind a FortiGate unit. The FortiGate unit intercepts the web traffic (HTTP and HTTPS) and caches pages from the web server. Reverse proxy web caching on the FortiGate unit reduces the number of requests that the web server must handle, leaving it free to process new requests that it has not serviced before.

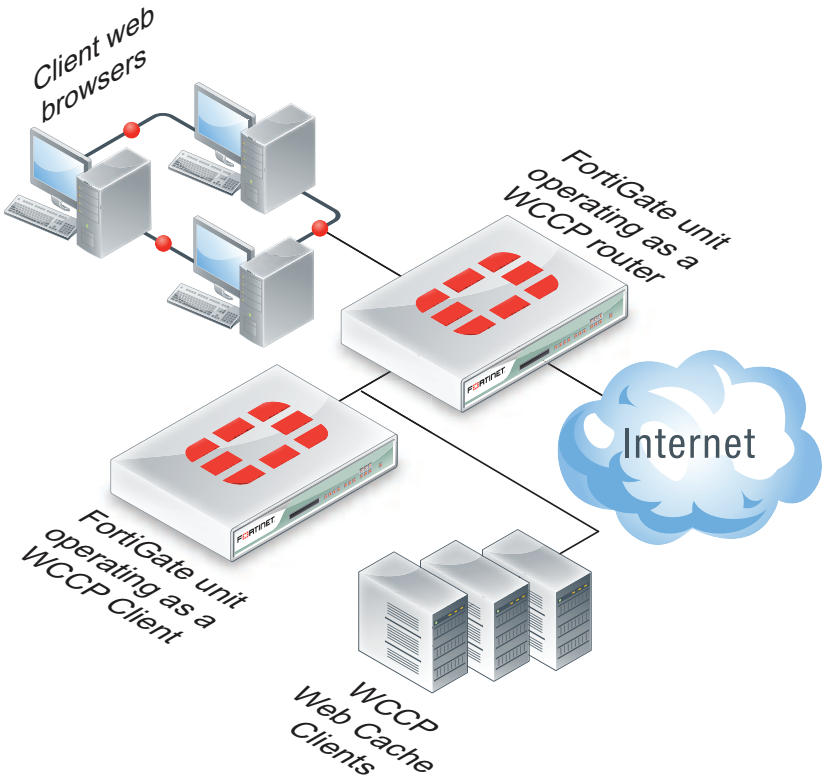
Reverse proxy web caching topology



WCCP topologies

You can operate a FortiGate unit as a Web Cache Communication Protocol (WCCP) router or cache engine. As a router, the FortiGate unit intercepts web browsing requests from client web browsers and forwards them to a WCCP cache engine. The cache engine returns the required cached content to the client web browser. If the cache server does not have the required content it accesses the content, caches it and returns the content to the client web browser.

WCCP topology



FortiGate units can also operate as WCCP cache servers, communicating with WCCP routers, caching web content and providing it to client web browsers as required.

WCCP is transparent to client web browsers. The web browsers do not have to be configured to use a web proxy.

Configuring WAN optimization

This chapter describes FortiGate WAN optimization client server architecture and other concepts you need to understand to be able to configure FortiGate WAN optimization.

Client/server architecture

Traffic across a WAN typically consists of clients on a client network communicating across a WAN with a remote server network. The clients do this by starting communication sessions from the client network to the server network. These communication sessions can be open text over the WAN or they can be encrypted by SSL VPN or IPsec VPN.

To optimize these sessions, you can add **WAN optimization security policies** to the **client-side FortiGate unit** to accept sessions from the client network that are destined for the server network. The client-side FortiGate unit is located between the client network and the WAN. WAN optimization security policies include **WAN optimization profiles** that control how the traffic is optimized.

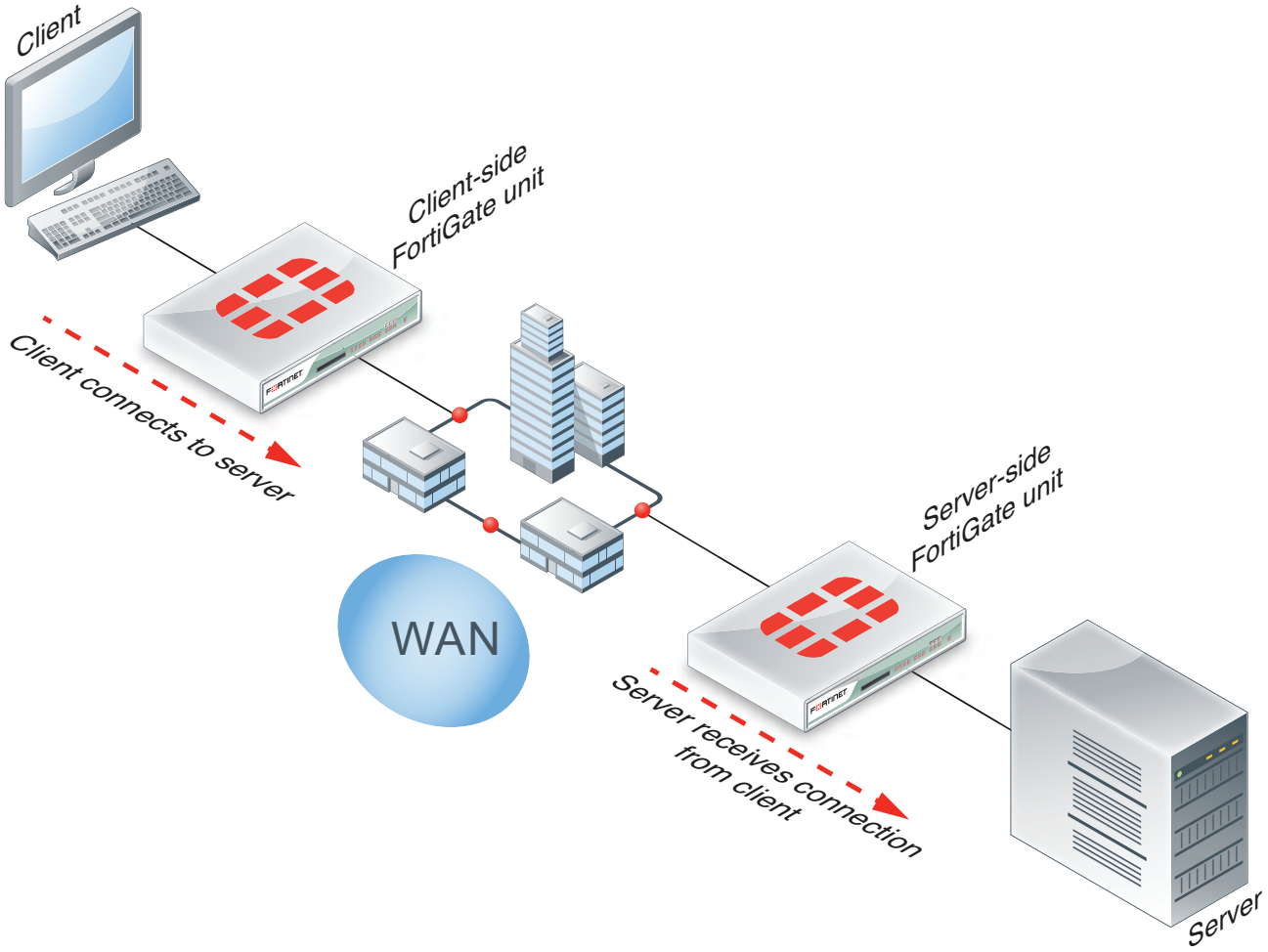
These same security policies can also include security profiles that apply UTM and NGFW features to WAN Optimization traffic.

The client-side FortiGate unit must also include the IP address of the **server-side FortiGate unit** in its WAN optimization **peer** configuration. The server-side FortiGate unit is located between the server network and the WAN, The peer configuration allows the client-side FortiGate unit to find the server-side FortiGate unit and attempt to establish a WAN optimization **tunnel** with it.

For the server-side FortiGate unit you must add a security policy with **wanopt** as the **Incoming Interface**. This security policy allows the FortiGate unit to accept WAN optimization sessions from the client-side FortiGate unit. For the server-side FortiGate unit to accept a WAN optimization connection it must have the client-side FortiGate unit in its WAN optimization peer configuration.

WAN optimization profiles are only added to the client-side WAN optimization security policy. The server-side FortiGate unit employs the WAN optimization settings set in the WAN optimization profile on the client-side FortiGate unit.

Client/server architecture



When both peers are identified the FortiGate units attempt to establish a WAN optimization **tunnel** between them. WAN optimization tunnels use port 7810. All optimized data flowing across the WAN between the client-side and server-side FortiGate units use this tunnel. WAN optimization tunnels can be encrypted use SSL encryption to keep the data in the tunnel secure.

Any traffic can be sent through a WAN optimization tunnel. This includes SSL and IPsec VPN traffic. However, instead of configuring SSL or IPsec VPN for this communication you can add SSL encryption using the WAN optimization tunnel.

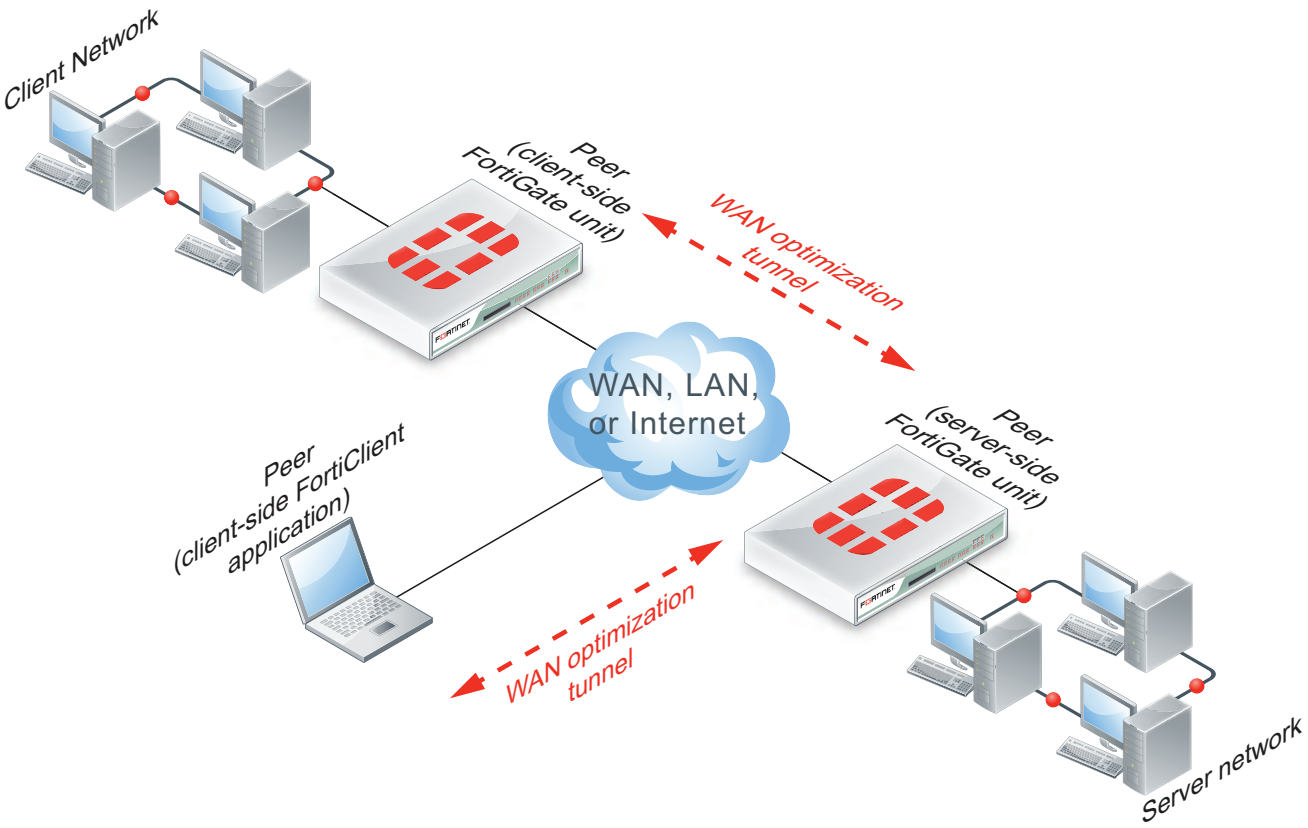
In addition to basic identification by peer host ID and IP address you can configure WAN optimization **authentication** using certificates and pre-shared keys to improve security. You can also configure FortiGate units involved in WAN optimization to accept connections from any identified peer or restrict connections to specific peers.

The FortiClient application can act in the same manner as a client-side FortiGate unit to optimize traffic between a computer running FortiClient and a FortiGate unit.

WAN optimization peers

The client-side and server-side FortiGate units are called WAN optimization peers because all of the FortiGate units in a WAN optimization network have the same peer relationship with each other. The client and server roles just relate to how a session is started. Any FortiGate unit configured for WAN optimization can be a client-side and a server-side FortiGate unit at the same time, depending on the direction of the traffic. Client-side FortiGate units initiate WAN optimization sessions and server-side FortiGate units respond to the session requests. Any FortiGate unit can simultaneously be a client-side FortiGate unit for some sessions and a server-side FortiGate unit for others.

WAN optimization peer and tunnel architecture



To identify all of the WAN optimization peers that a FortiGate unit can perform WAN optimization with, you add host IDs and IP addresses of all of the peers to the FortiGate unit configuration. The peer IP address is actually the IP address of the peer unit interface that communicates with the FortiGate unit.

Manual (peer-to-peer) and active-passive WAN optimization

You can create **manual** (peer-to-peer) and **active-passive** WAN optimization configurations.

Manual (peer to peer) configurations

Manual configurations allow for WAN optimization between one client-side FortiGate unit and one server-side FortiGate unit. To create a manual configuration you add a **manual mode** WAN optimization security policy to

the client-side FortiGate unit. The manual mode policy includes the peer ID of a server-side FortiGate unit.

In a manual mode configuration, the client-side peer can only connect to the named server-side peer. When the client-side peer initiates a tunnel with the server-side peer, the packets that initiate the tunnel include extra information so that the server-side peer can determine that it is a peer-to-peer tunnel request. This extra information is required because the server-side peer does not require a WAN optimization policy; however, you need to add the client peer host ID and IP address to the server-side FortiGate unit peer list.

In addition, from the server-side FortiGate unit CLI you must and an Explicit Proxy security policy with `proxy` set to `wanopt` and the destination interface and network set to the network containing the servers that clients connect to over the WAN optimization tunnel. WAN optimization tunnel requests are accepted by the explicit proxy policy and if the client-side peer is in the server side peer's address list the traffic is forwarded to the servers on the destination network.

Manual mode client-side policy

You must configure manual mode client-side policies from the CLI. From the GUI a manual mode policy has WAN Optimization turned on and includes the following text beside the *WAN optimization* field: *Manual (Profile: <profile-name>. Peer: <peer-name>*.

Add a manual mode policy to the client-side FortiGate unit from the CLI. The policy enables WAN optimization, sets `wanopt-detection` to `off`, and uses the `wanopt-peer` option to specify the server-side peer. The following example uses the default WAN optimization profile.

```
config firewall policy
   edit 2
      set srcintf internal
      set dstintf wan1
      set srcaddr client-subnet
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
      set wanopt enable
      set wanopt-detection off
      set wanopt-profile default
      set wanopt-peer server
   next
end
```

Manual mode server-side explicit proxy policy

The server-side explicit proxy policy allows connections from the WAN optimization tunnel to the server network by setting the proxy type to `wanopt`. You must add policies that set `proxy` to `wanopt` from the CLI and these policies do not appear on the GUI. The policy should look like the following:

```
configure firewall explicit-proxy-policy
   edit 3
      set proxy wanopt
      set dstintf internal
      set srcaddr all
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
   next
```

```
end
```

Active-passive configurations

Active-passive WAN optimization requires an **active** WAN optimization policy on the client-side FortiGate unit and a **passive** WAN optimization policy on the server-side FortiGate unit. The server-side FortiGate unit also requires an explicit proxy policy with `proxy` set to `wanopt`.

You can use the passive policy to control WAN optimization address translation by specifying **transparent mode** or non-transparent mode. SeeWAN optimization transparent mode on page 2835. You can also use the passive policy to apply security profiles, web caching, and other FortiGate features at the server-side FortiGate unit. For example, if a server-side FortiGate unit is protecting a web server, the passive policy could enable web caching.

A single passive policy can accept tunnel requests from multiple FortiGate units as long as the server-side FortiGate unit includes their peer IDs and all of the client-side FortiGate units include the server-side peer ID.

Active client-side policy

Add an active policy to the client-side FortiGate unit by turning on **WAN Optimization** and selecting **active**. Then select a WAN optimization **Profile.** From the CLI the policy could look like the following:

```
config firewall policy
   edit 2
      set srcintf internal
      set dstintf wan1
      set srcaddr client-subnet
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
      set wanopt enable
      set wanopt-detection active
      set wanopt-profile default
   next
end
```

Server-side tunnel policy

The server-side requires an explicit proxy policy that sets the `proxy` to `wanopt`. You must add this policy from the CLI and policies with `proxy` set to `wanopt` do not appear on the GUI. From the CLI the policy could look like the following:

```
configure firewall explicit-proxy-policy
   edit 3
      set proxy wanopt
      set dstintf internal
      set srcaddr all
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
   next
end
```

Server-side passive policy

Add a passive policy to the server-side FortiGate unit by selecting **Enable WAN Optimization** and selecting **passive**. Then set the **Passive Option** to **transparent**. From the CLI the policy could look like the following:

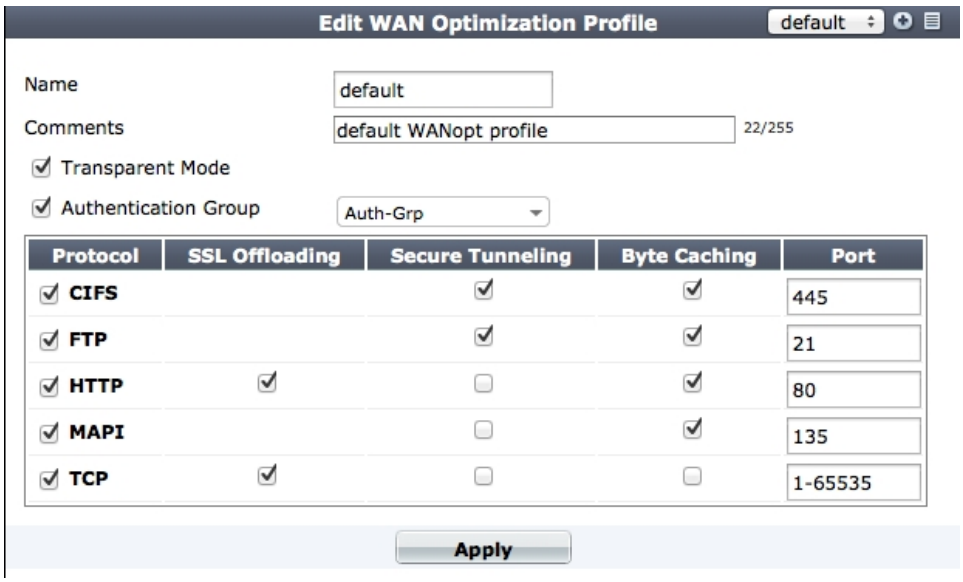
```
config firewall policy
edit 2
      set srcintf "wan1"
      set dstintf "internal"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set wanopt enable
      set wanopt-detection passive
      set wanopt-passive-opt transparent
   next
```

WAN optimization profiles

Use WAN optimization profiles to apply WAN optimization techniques to traffic to be optimized. In a WAN optimization profile you can select the protocols to be optimized and for each protocol you can enable SSL offloading (if supported), secure tunneling, byte caching and set the port or port range the protocol uses. You can also enable transparent mode and optionally select an authentication group. You can edit the default WAN optimization profile or create new ones.

To configure a WAN optimization profile go to **WAN Opt & Cache > WAN Opt. Profile > Profiles** and edit a profile or create a new one.

Configuring a WAN optimization profile



From the CLI you can use the following command to configure a WAN optimization profile to optimize HTTP traffic.

```
config wanopt profile
   edit new-profile
      config http
         set status enable
   end
```

Transparent Mode	Servers receiving packets after WAN optimization “see” different source addresses depending on whether or not you select **Transparent Mode**. For more information, see WAN optimization transparent mode on page 2835.
Authentication Group	Select this option and select an authentication group so that the client and server-side FortiGate units must authenticate with each other before starting the WAN optimization tunnel. You must also select an authentication group if you select **Secure Tunneling** for any protocol. You must add identical authentication groups to both of the FortiGate units that will participate in the WAN optimization tunnel. For more information, see Configuring authentication groups on page 2847.
Protocol	Select CIFS, FTP, HTTP or MAPI to apply protocol optimization for the selected protocols. See Protocol optimization on page 2833. Select TCP if the WAN optimization tunnel accepts sessions that use more than one protocol or that do not use the CIFS, FTP, HTTP, or MAPI protocol.
SSL Offloading	Select to apply SSL offloading for HTTPS or other SSL traffic. You can use SSL offloading to offload SSL encryption and decryption from one or more HTTP servers to the FortiGate unit. If you enable this option, you must configure the security policy to accept SSL-encrypted traffic. If you enable SSL offloading, you must also use the CLI command `config firewall ssl-server` to add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for. For more information, see Turning on web caching for HTTPS traffic on page 2876.
Secure Tunnelling	The WAN optimization tunnel is encrypted using SSL encryption. You must also add an authentication group to the profile. For more information, see Secure tunneling on page 2849.
Byte Caching	Select to apply WAN optimization byte caching to the sessions accepted by this rule. For more information, see “Byte caching”.
Port	Enter a single port number or port number range. Only packets whose destination port number matches this port number or port number range will be optimized.

Processing non-HTTP sessions accepted by a WAN optimization profile with HTTP optimization

From the CLI, you can use the following command to configure how to process non-HTTP sessions when a rule configured to accept and optimize HTTP traffic accepts a non-HTTP session. This can occur if an application sends non-HTTP sessions using an HTTP destination port.

```
config wanopt profile
   edit default
      config http
         set status enable
         set tunnel-non-http {disable | enable}
      end
```

To drop non-HTTP sessions accepted by the rule set `tunnel-non-http` to `disable`, or set it to `enable` to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. In this case, the FortiGate unit applies TCP protocol optimization to non-HTTP sessions.

Processing unknown HTTP sessions

Unknown HTTP sessions are HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1. From the CLI, use the following command to specify how a rule handles such HTTP sessions.

```
config wanopt profile
   edit default
      config http
         set status enable
         set unknown-http-version {best-effort | reject | tunnel}
      end
```

To assume that all HTTP sessions accepted by the rule comply with HTTP 0.9, 1.0, or 1.1, select `best-effort`. If a session uses a different HTTP version, WAN optimization may not parse it correctly. As a result, the FortiGate unit may stop forwarding the session and the connection may be lost. To reject HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1, select `reject`.

To pass HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1, but without applying HTTP protocol optimization, byte-caching, or web caching, you can also select `tunnel`. TCP protocol optimization is applied to these HTTP sessions.

Protocol optimization

Protocol optimization techniques optimize bandwidth use across the WAN. These techniques can improve the efficiency of communication across the WAN optimization tunnel by reducing the amount of traffic required by communication protocols. You can apply protocol optimization to Common Internet File System (CIFS), FTP, HTTP, MAPI, and general TCP sessions. You can apply general TCP optimization to MAPI sessions.

For example, CIFS provides file access, record locking, read/write privileges, change notification, server name resolution, request batching, and server authentication. CIFS is a fairly “chatty” protocol, requiring many background transactions to successfully transfer a single file. This is usually not a problem across a LAN. However, across a WAN, latency and bandwidth reduction can slow down CIFS performance.

When you select the CIFS protocol in a WAN optimization profile, the FortiGate units at both ends of the WAN optimization tunnel use a number of techniques to reduce the number of background transactions that occur over the WAN for CIFS traffic.

If a policy accepts a range of different types of traffic, you can set **Protocol** to **TCP** to apply general optimization techniques to TCP traffic. However, applying this TCP optimization is not as effective as applying more protocol-specific optimization to specific types of traffic. TCP protocol optimization uses techniques such as TCP SACK support, TCP window scaling and window size adjustment, and TCP connection pooling to remove TCP bottlenecks.

Protocol optimization and MAPI

By default the MAPI service uses port number 135 for RPC port mapping and may use random ports for MAPI messages. The random ports are negotiated through sessions using port 135. The FortiOS DCE-RPC session helper learns these ports and opens pinholes for the messages. WAN optimization is also aware of these ports and attempts to apply protocol optimization to MAPI messages that use them. However, to configure protocol optimization for MAPI you should set the WAN optimization profile to a single port number (usually port 135). Specifying a range of ports may reduce performance.

Byte caching

Byte caching breaks large units of application data (for example, a file being downloaded from a web page) into small chunks of data, labelling each chunk of data with a hash of the chunk and storing those chunks and their hashes in a database. The database is stored on a WAN optimization storage device. Then, instead of sending the actual data over the WAN tunnel, the FortiGate unit sends the hashes. The FortiGate unit at the other end of the tunnel receives the hashes and compares them with the hashes in its local byte caching database. If any hashes match, that data does not have to be transmitted over the WAN optimization tunnel. The data for any hashes that does not match is transferred over the tunnel and added to that byte caching database. Then the unit of application data (the file being downloaded) is reassembled and sent to its destination.

The stored byte caches are not application specific. Byte caches from a file in an email can be used to optimize downloading that same file or a similar file from a web page.

The result is less data transmitted over the WAN. Initially, byte caching may reduce performance until a large enough byte caching database is built up.

To enable byte caching, you select **Byte Caching** in a WAN optimization profile.

Byte caching cannot determine whether or not a file is compressed (for example a zip file), and caches compressed and non-compressed versions of the same file separately.

Dynamic data chunking for byte caching

Dynamic data chunking can improve byte caching by improving detection of data chunks that are already cached in changed files or in data embedded in traffic using an unknown protocol. Dynamic data chunking is available for HTTP, CIFS and FTP.

Use the following command to enable dynamic data chunking for HTTP in the default WAN optimization profile.

```
config wanopt profile
   edit default
        config http
           set prefer-chunking dynamic
      end
```

By default dynamic data chunking is disabled and `prefer-chunking` is set to `fix`.

WAN optimization transparent mode

WAN optimization is transparent to users. This means that with WAN optimization in place, clients connect to servers in the same way as they would without WAN optimization. However, servers receiving packets after WAN optimization "see" different source addresses depending on whether or not transparent mode is selected for WAN optimization. If transparent mode is selected, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be configured to route traffic with client source IP addresses from the server-side FortiGate unit to the server and back to the server-side FortiGate unit.

Some protocols, for example CIFS, may not function as expected if transparent mode is **not** selected. In most cases, for CIFS WAN optimization you should select transparent mode and make sure the server network can route traffic as described to support transparent mode.

If transparent mode is not selected, the source address of the packets received by servers is changed to the address of the server-side FortiGate unit interface that sends the packets to the servers. So servers appear to receive packets from the server-side FortiGate unit. Routing on the server network is simpler in this case because client addresses are not involved. All traffic appears to come from the server-side FortiGate unit and not from individual clients.

Do not confuse WAN optimization transparent mode with FortiGate transparent mode. WAN optimization transparent mode is similar to source NAT. FortiGate Transparent mode is a system setting that controls how the FortiGate unit (or a VDOM) processes traffic.

Configuring Transparent mode

You can configure transparent mode by selecting **Transparent** in a WAN Optimization profile. The profile is added to an active WAN Optimization policy.

When you configure a passive WAN Optmization policy you can accept the active policy transparent setting or you can override the active policy transparent setting. From the GUI you can do this by setting the **Passive Option** as follows:

- **default** use the transparent setting in the WAN Optimization profile added to the active policy (client-side configuration).
- **transparent** impose transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate keep their original source addresses.
- **non-transparent** impose non-transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate have their source address changed to the address of the server-side FortiGate unit interface that sends the packets to the servers.

From the CLI you can use the following command:

```
config firewall policy
   set wanopt-passive-opt {default | transparent | non-transparent}
end
```

FortiClient WAN optimization

PCs running the FortiClient application are client-side peers that initiate WAN optimization tunnels with server-side peer FortiGate units. However, you can have an ever-changing number of FortiClient peers with IP addresses that also change regularly. To avoid maintaining a list of such peers, you can instead configure WAN optimization to accept any peer and use authentication to identify FortiClient peers.

Together, the WAN optimization peers apply the WAN optimization features to optimize the traffic flow over the WAN between the clients and servers. WAN optimization reduces bandwidth requirements, increases throughput, reduces latency, offloads SSL encryption/decryption and improves privacy for traffic on the WAN.

For more details, see FortiClient WAN optimization on page 2893.

Operating modes and VDOMs

To use WAN optimization, the FortiGate units can operate in either NAT/Route or Transparent mode. The client-side and server-side FortiGate units do not have to be operating in the same mode.

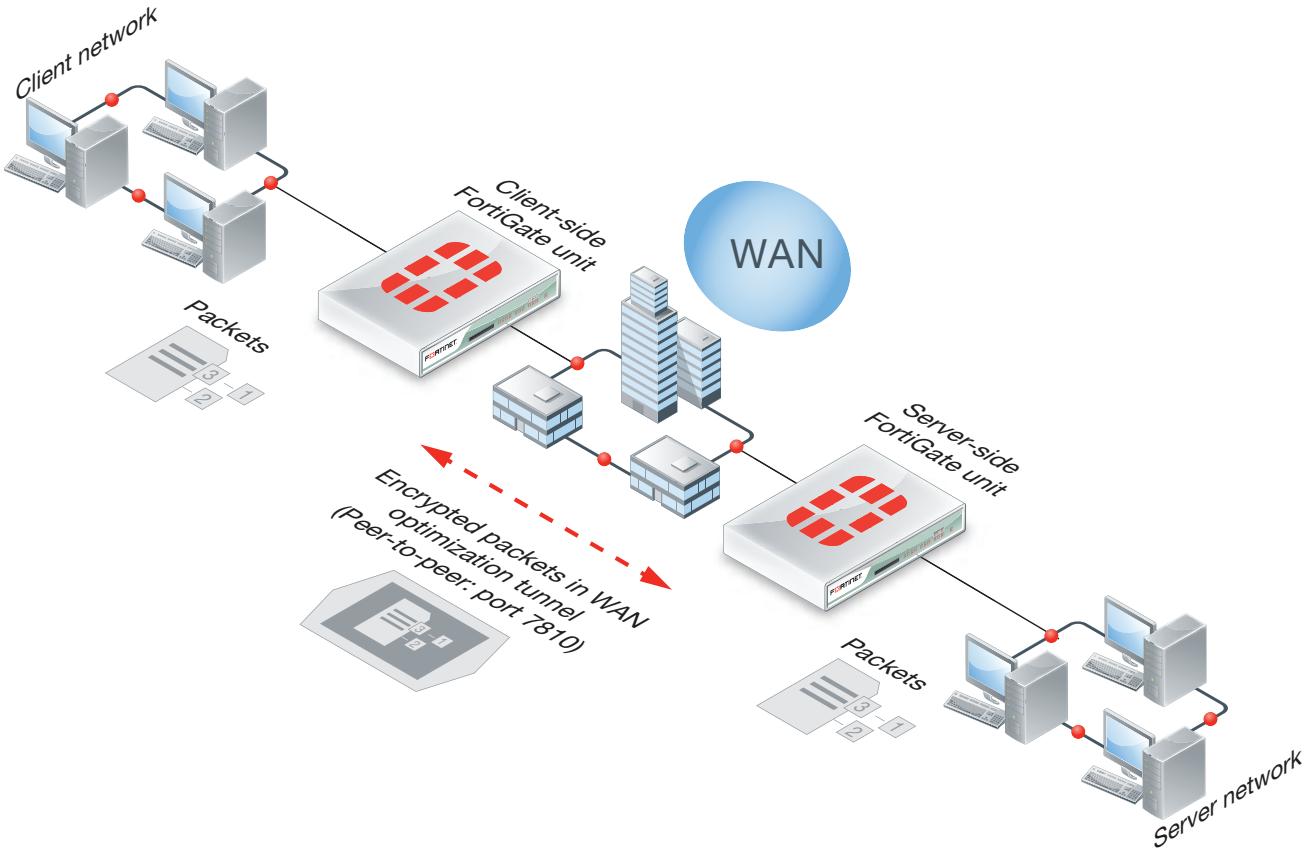
As well, the FortiGate units can be configured for multiple virtual domain (VDOM) operation. You configure WAN optimization for each VDOM and configure one or both of the units to operate with multiple VDOMs enabled.

If a FortiGate unit or VDOM is operating in Transparent mode with WAN optimization enabled, WAN optimization uses the management IP address as the peer IP address of the FortiGate unit instead of the address of an interface.

WAN optimization tunnels

All optimized traffic passes between the FortiGate units or between a FortiClient peer and a FortiGate unit over a WAN optimization tunnel. Traffic in the tunnel can be sent in plain text or encrypted using AES-128bit-CBC SSL.

WAN optimization tunnels



Both plain text and the encrypted tunnels use TCP destination port 7810.

Before a tunnel can be started, the peers must be configured to authenticate with each other. Then, the client-side peer attempts to start a WAN optimization tunnel with the server-side peer. Once the peers authenticate with each other, they bring up the tunnel and WAN optimization communication over the tunnel starts. After a tunnel has been established, multiple WAN optimization sessions can start and stop between peers without restarting the tunnel.

Tunnel sharing

You can use the `tunnel-sharing` WAN optimization profile CLI keyword to configure tunnel sharing for WAN optimization rules. Tunnel sharing means multiple WAN optimization sessions share the same tunnel. Tunnel sharing can improve performance by reducing the number of WAN optimization tunnels between FortiGate units. Having fewer tunnels means less data to manage. Also, tunnel setup requires more than one exchange of information between the ends of the tunnel. Once the tunnel is set up, each new session that shares the tunnel avoids tunnel setup delays.

Tunnel sharing also uses bandwidth more efficiently by reducing the chances that small packets will be sent down the tunnel. Processing small packets reduces network throughput, so reducing the number of small packets improves performance. A shared tunnel can combine all the data from the sessions being processed by the tunnel and send the data together. For example, suppose a FortiGate unit is processing five WAN optimization sessions and each session has 100 bytes to send. If these sessions use a shared tunnel, WAN optimization combines the

packets from all five sessions into one 500-byte packet. If each session uses its own private tunnel, five 100-byte packets will be sent instead. Each packet also requires a TCP ACK reply. The combined packet in the shared tunnel requires one TCP ACK packet. The separate packets in the private tunnels require five.

Use the following command to configure tunnel sharing for HTTP traffic in a WAN optimization profile.

```
config wanopt profile
   edit default
      config http
         set tunnel-sharing {express-shared | private | shared}
      end
```

Tunnel sharing is not always recommended and may not always be the best practice. Aggressive and non-aggressive protocols should not share the same tunnel. An aggressive protocol can be defined as a protocol that is able to get more bandwidth than a non-aggressive protocol. (The aggressive protocols can “starve” the non-aggressive protocols.) HTTP and FTP are considered aggressive protocols. If aggressive and non-aggressive protocols share the same tunnel, the aggressive protocols may take all of the available bandwidth. As a result, the performance of less aggressive protocols could be reduced. To avoid this problem, rules for HTTP and FTP traffic should have their own tunnel. To do this, set `tunnel-sharing` to `private` for WAN optimization rules that accept HTTP or FTP traffic.

It is also useful to set `tunnel-sharing` to `express-shared` for applications, such as Telnet, that are very interactive but not aggressive. Express sharing optimizes tunnel sharing for Telnet and other interactive applications where latency or delays would seriously affect the user’s experience with the protocol.

Set `tunnel-sharing` to `shared` for applications that are not aggressive and are not sensitive to latency or delays. WAN optimization rules set to `sharing` and `express-shared` can share the same tunnel.

WAN optimization and user and device identity policies, load balancing and traffic shaping

Please note the following about WAN optimization and firewall policies:

- WAN optimization is not compatible with firewall load balancing.
- WAN optimization is compatible with source and destination NAT options in firewall policies (including firewall virtual IPs). If a virtual IP is added to a policy the traffic that exits the WAN optimization tunnel has its destination address changed to the virtual IPs mapped to IP address and port.
- WAN optimization is compatible with user identity-based and device identity security policies. If a session is allowed after authentication or device identification the session can be optimized.

Traffic shaping

Traffic shaping works for WAN optimization traffic that is not in a WAN optimization tunnel. So traffic accepted by a WAN optimization security policy on a client-side FortiGate unit can be shaped on ingress. However, when the traffic enters the WAN optimization tunnel, traffic shaping is not applied.

In manual mode:

- Traffic shaping works as expected on the client-side FortiGate unit.
- Traffic shaping cannot be applied to traffic on the server-side FortiGate unit.

In active-passive mode:

- Traffic shaping works as expected on the client-side FortiGate unit.
- If transparent mode is enabled in the WAN optimization profile, traffic shaping also works as expected on the

server-side FortiGate unit.

- If transparent mode is not enabled, traffic shaping works partially on the server-side FortiGate unit.

WAN optimization and HA

You can configure WAN optimization on a FortiGate HA cluster. The recommended best practice HA configuration for WAN optimization is active-passive mode. When the cluster is operating, all WAN optimization sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance WAN optimization sessions.

You can also form a WAN optimization tunnel between a cluster and a standalone FortiGate unit or between two clusters.

In a cluster, only the primary unit stores the byte cache database. This database is not synchronized to the subordinate units. So, after a failover, the new primary unit must rebuild its byte cache. Rebuilding the byte cache can happen relatively quickly because the new primary unit gets byte cache data from the other FortiGate unit that it is participating with in WAN optimization tunnels.

WAN optimization, web caching and memory usage

To accelerate and optimize disk access and to provide better throughput and less latency FortiOS WAN optimization uses provisioned memory to reduce disk I/O and increase disk I/O efficiency. In addition, WAN optimization requires a small amount of additional memory per session for comprehensive flow control logic and efficient traffic forwarding.

When WAN optimization is enabled you will see a reduction in available memory. The reduction increases when more WAN optimization sessions are being processed. If you are thinking of enabling WAN optimization on an operating FortiGate unit, make sure its memory usage is not maxed out during high traffic periods.

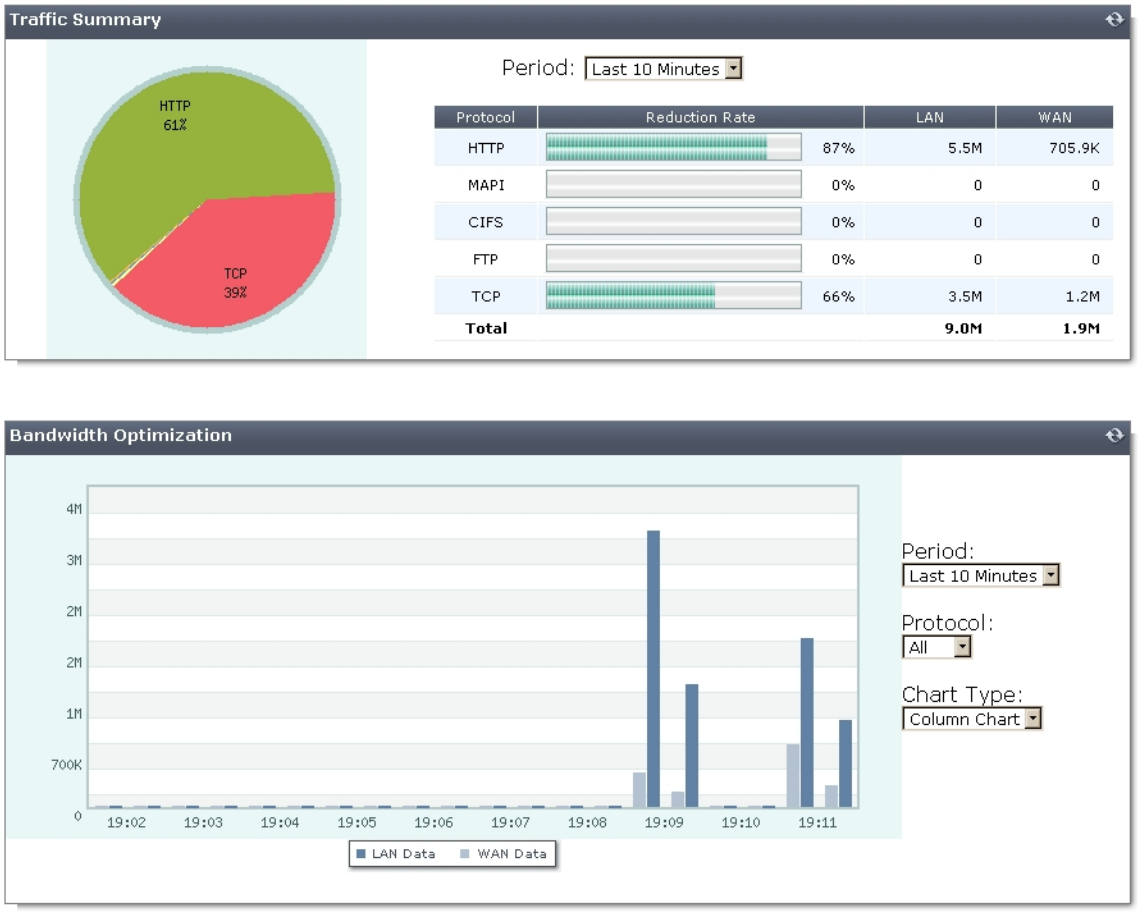
In addition to using the system dashboard to see the current memory usage you can use the `get test wad 2` command to see how much memory is currently being used by WAN optimization. See "get test {wad | wccpd} <test_level>" for more information.

Monitoring WAN optimization performance

Using WAN optimization monitoring, you can confirm that a FortiGate unit is optimizing traffic and view estimates of the amount of bandwidth saved. The WAN optimization monitor presents collected log information in a graphical format to show network traffic summary and bandwidth optimization information.

To view the WAN optimization monitor, go to **WAN Opt. & Cache > Monitor > WAN Opt Monitor**.

WAN optimization monitor



Traffic Summary

The traffic summary shows how WAN optimization is reducing the amount of traffic on the WAN for each WAN optimization protocol by showing the traffic reduction rate as a percentage of the total traffic. The traffic summary also shows the amount of WAN and LAN traffic. If WAN optimization is being effective the amount of WAN traffic should be lower than the amount of LAN traffic.

You can use the refresh icon to update the traffic summary display at any time. You can also set the amount of time for which the traffic summary shows data. The time period can vary from the last 10 minutes to the last month.

Bandwidth Optimization

This section shows network bandwidth optimization per time period. A line or column chart compares an application's pre-optimized size (LAN data) with its optimized size (WAN data). You can select the chart type, the monitoring time period, and the protocol for which to display data. If WAN optimization is being effective the WAN bandwidth should be lower than the LAN bandwidth.

WAN optimization configuration summary

This section includes a client-side and a server-side WAN Optimization configuration summary.:

Client-side configuration summary

WAN optimization profile

Enter the following command to view WAN optimization profile CLI options:

```
tree wanopt profile
-- [profile] --*name (36)
      |- transparent
      |- comments
      |- auth-group (36)
      |- <http> -- status
            |- secure-tunnel
            |- byte-caching
            |- prefer-chunking
            |- tunnel-sharing
            |- log-traffic
            |- port (1,65535)
            |- ssl
            |- ssl-port (1,65535)
            |- unknown-http-version
            +- tunnel-non-http
      |- <cifs> -- status
            |- secure-tunnel
            |- byte-caching
            |- prefer-chunking
            |- tunnel-sharing
            |- log-traffic
            +- port (1,65535)
      |- <mapi> -- status
            |- secure-tunnel
            |- byte-caching
            |- tunnel-sharing
            |- log-traffic
            +- port (1,65535)
      |- <ftp> -- status
            |- secure-tunnel
            |- byte-caching
            |- prefer-chunking
            |- tunnel-sharing
            |- log-traffic
            +- port (1,65535)
      +- <tcp> -- status
            |- secure-tunnel
            |- byte-caching
            |- byte-caching-opt
            |- tunnel-sharing
            |- log-traffic
            |- port
            |- ssl
            +- ssl-port (1,65535)
```

Local host ID and peer settings

```
config wanopt settings
   set host-id client
end
config wanopt peer
   edit server
   set ip 10.10.2.82
end
```

Security policies

Two client-side WAN optimization security policy configurations are possible. One for active-passive WAN optimization and one for manual WAN optimization.

Active/passive mode on the client-side

```
config firewall policy
   edit 2
      set srcintf internal
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set wanopt enable <<< enable WAN optimization
      set wanopt-detection active <<< set the mode to active/passive
      set wanopt-profile "default" <<< select the wanopt profile
   next
end
```

Manual mode on the client-side

```
config firewall policy
   edit 2
      set srcintf internal
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set wanopt enable <<< enable WAN optimization
      set wanopt-detection off <<< sets the mode to manual
      set wanopt-profile "default" <<< select the wanopt profile
      set wanopt-peer "server" <<< set the only peer to do wanopt
                                                    with (required for manual mode)
   next
end
```

server-side configuration summary

Local host ID and peer settings

```
config wanopt settings
   set host-id server
end
config wanopt peer
   edit client
      set ip 10.10.2.81
end
```

Security policies

Two server-side WAN optimization security policy configurations are possible. One for active-passive WAN optimization and one for manual WAN optimization.

Active/passive mode on server-side

```
config firewall policy
edit 2 <<< the passive mode policy
      set srcintf wan1
      set dstintf internal
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set wanopt enable
      set wanopt-detection passive
      set wanopt-passive-opt transparent
   end
config firewall explicit-proxy-policy
   edit 3 <<< policy that accepts wanopt tunnel connections from the server
      set proxy wanopt <<< wanopt proxy type
      set dstintf internal
      set srcaddr all
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
   next
end
```

Manual mode on server-side

```
config firewall explicit-proxy-policy
   edit 3 <<< policy that accepts wanopt tunnel connections from the client
      set proxy wanopt <<< wanopt proxy type
      set dstintf internal
      set srcaddr all
      set dstaddr server-subnet
      set action accept
      set schedule always
      set service ALL
```

```
    next
end
```

Best practices

This is a short list of WAN optimization and explicit proxy best practices.

- WAN optimization tunnel sharing is recommended for similar types of WAN optimization traffic. However, tunnel sharing for different types of traffic is not recommended. For example, aggressive and non-aggressive protocols should not share the same tunnel. See Tunnel sharing on page 2837.
- Active-passive HA is the recommended HA configuration for WAN optimization. See WAN optimization and HA on page 2839.
- Configure WAN optimization authentication with specific peers. Accepting any peer is not recommended as this can be less secure. SeeAccepting any peers on page 2845.
- Set the explicit proxy **Default Firewall Policy Action** to **Deny**. This means that a security policy is required to use the explicit web proxy. See The FortiGate explicit web proxy on page 2897.
- Set the explicit FTP proxy **Default Firewall Policy Action** to **Deny**. This means that a security policy is required to use the explicit FTP proxy. See General explicit FTP proxy configuration steps on page 2926.
- Do not enable the explicit web or FTP proxy on an interface connected to the Internet. This is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address. If you must enable the proxy on such an interface make sure authentication is required to use the proxy. See General explicit web proxy configuration steps on page 2899.

Peers and authentication groups

All communication between WAN optimization peers begins with one WAN optimization peer (or client-side FortiGate unit) sending a WAN optimization tunnel request to another peer (or server-side FortiGate unit). During this process, the WAN optimization peers identify and optionally authenticate each other.

Basic WAN optimization peer requirements

WAN optimization requires the following configuration on each peer. For information about configuring local and peer host IDs, see Configuring peers on page 2846.

- The peer must have a unique host ID.
- Unless authentication groups are used, peers authenticate each other using host ID values. Do not leave the local host ID at its default value.
- The peer must know the host IDs and IP addresses of all of the other peers that it can start WAN optimization tunnels with. This does not apply if you use authentication groups that accept all peers.
- All peers must have the same local certificate installed on their FortiGate units if the units authenticate by local certificate. Similarly, if the units authenticate by pre-shared key (password), administrators must know the password. The type of authentication is selected in the authentication group. This applies only if you use authentication groups.

Accepting any peers

Strictly speaking, you do not need to add peers. Instead you can configure authentication groups that accept any peer. However, for this to work, both peers must have the same authentication group (with the same name) and both peers must have the same certificate or pre-shared key.

Accepting any peer is useful if you have many peers or if peer IP addresses change. For example, you could have many travelling FortiClient peers with IP addresses that are always changing as the users travel to different customer sites. This configuration is also useful if you have FortiGate units with dynamic external IP addresses (using DHCP or PPPoE). For most other situations, this method is not recommended and is not a best practice as it is less secure than accepting defined peers or a single peer. For more information, see Configuring authentication groups on page 2847.

How FortiGate units process tunnel requests for peer authentication

When a client-side FortiGate unit attempts to start a WAN optimization tunnel with a peer server-side FortiGate unit, the tunnel request includes the following information:

- the client-side local host ID
- the name of an authentication group, if included in the rule that initiates the tunnel
- if an authentication group is used, the authentication method it specifies: pre-shared key or certificate
- the type of tunnel (secure or not).

For information about configuring the local host ID, peers and authentication groups, see Configuring peers on page 2846 and Configuring authentication groups on page 2847.

The authentication group is optional unless the tunnel is a secure tunnel. For more information, see Secure tunneling on page 2849.

If the tunnel request includes an authentication group, the authentication will be based on the settings of this group as follows:

- The server-side FortiGate unit searches its own configuration for the name of the authentication group in the tunnel request. If no match is found, the authentication fails.
- If a match is found, the server-side FortiGate unit compares the authentication method in the client and server authentication groups. If the methods do not match, the authentication fails.
- If the authentication methods match, the server-side FortiGate unit tests the peer acceptance settings in its copy of the authentication group.
- If the setting is **Accept Any Peer**, the authentication is successful.
- If the setting is **Specify Peer**, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the peer name in the server-side authentication group. If the names match, authentication is successful. If a match is not found, authentication fails.
- If the setting is **Accept Defined Peers**, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the server-side peer list. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the tunnel request does not include an authentication group, authentication will be based on the client-side local host ID in the tunnel request. The server-side FortiGate unit searches its peer list to match the client-side local host ID in the tunnel request. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the server-side FortiGate unit successfully authenticates the tunnel request, the server-side FortiGate unit sends back a tunnel setup response message. This message includes the server-side local host ID and the authentication group that matches the one in the tunnel request.

The client-side FortiGate unit then performs the same authentication procedure as the server-side FortiGate unit did. If both sides succeed, tunnel setup continues.

Configuring peers

When you configure peers, you first need to add the local host ID that identifies the FortiGate unit for WAN optimization and then add the peer host ID and IP address of each FortiGate unit with which a FortiGate unit can create WAN optimization tunnels.

To configure WAN optimization peers - web-based manager:

1. Go to **Wan Opt. & Cache > WAN Opt. Peers > Peers**.
2. For **Local Host ID**, enter the local host ID of **this** FortiGate unit and select **Apply**. If you add this FortiGate unit as a peer to another FortiGate unit, use this ID as its **peer** host ID.

   The local or host ID can contain up to 25 characters and can include spaces.
3. Select **Create New** to add a new peer.
4. For **Peer Host ID**, enter the peer host ID of the peer FortiGate unit. This is the local host ID added to the peer FortiGate unit.
5. For **IP Address**, add the IP address of the peer FortiGate unit. This is the source IP address of tunnel requests sent by the peer, usually the IP address of the FortiGate interface connected to the WAN.
6. Select **OK**.

To configure WAN optimization peers - CLI:

In this example, the local host ID is named `HQ_Peer` and has an IP address of `172.20.120.100`. Three peers are added, but you can add any number of peers that are on the WAN.

1. Enter the following command to set the local host ID to `HQ_Peer`.

```
config wanopt settings
   set host-id HQ_peer
end
```

2. Enter the following commands to add three peers.

```
config wanopt peer
   edit Wan_opt_peer_1
      set ip 172.20.120.100
   next
   edit Wan_opt_peer_2
      set ip 172.30.120.100
   next
   edit Wan_opt_peer_3
      set ip 172.40.120.100
   end
```

Configuring authentication groups

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers.

To perform authentication, WAN optimization peers use a certificate or a pre-shared key added to an authentication group so they can identify each other before forming a WAN optimization tunnel. Both peers must have an authentication group with the same name and settings. You add the authentication group to a peer-to-peer or active rule on the client-side FortiGate unit. When the server-side FortiGate unit receives a tunnel start request from the client-side FortiGate unit that includes an authentication group, the server-side FortiGate unit finds an authentication group in its configuration with the same name. If both authentication groups have the same certificate or pre-shared key, the peers can authenticate and set up the tunnel.

Authentication groups are also required for secure tunneling.

To add authentication groups, go to **WAN Opt. & Cache > WAN Opt. Peers > Authentication Groups**.

To add an authentication group - web-based manager:

Use the following steps to add any kind of authentication group. It is assumed that if you are using a local certificate to authenticate, it is already added to the FortiGate unit

1. Go to **Wan Opt. & Cache > WAN Opt. Peers > Authentication Groups**.
2. Select **Create New**.
3. Add a **Name** for the authentication group.

   You will select this name when you add the authentication group to a WAN optimization rule.
4. Select the **Authentication Method**.

   Select **Certificate** if you want to use a certificate to authenticate and encrypt WAN optimization tunnels. You must select a local certificate that has been added to this FortiGate unit. (To add a local certificate, go to **System > Certificates > Local Certificates**.) Other FortiGate units that participate in WAN optimization tunnels with this

FortiGate unit must have an authentication group with the same name and certificate.

Select **Pre-shared key** if you want to use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels. You must add the **Password** (or pre-shared key) used by the authentication group. Other FortiGate units that participate in WAN optimization tunnels with this FortiGate unit must have an authentication group with the same name and password. The password must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

5. Configure **Peer Acceptance** for the authentication group.

   Select **Accept Any Peer** if you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP.

   Select **Accept Defined Peers** if you want to authenticate with peers added to the peer list only.

   Select **Specify Peer** and select one of the peers added to the peer list to authenticate with the selected peer only.

6. Select **OK**.
7. Add the authentication group to a WAN optimization rule to apply the authentication settings in the authentication group to the rule.

To add an authentication group that uses a certificate- CLI:

Enter the following command to add an authentication group that uses a certificate and can authenticate all peers added to the FortiGate unit configuration.

In this example, the authentication group is named `auth_grp_1` and uses a certificate named `Example_Cert`.

```
config wanopt auth-group
   edit auth_grp_1
      set auth-method cert
      set cert Example_Cert
      set peer-accept defined
   end
```

To add an authentication group that uses a pre-shared key - CLI:

Enter the following command to add an authentication group that uses a pre-shared key and can authenticate only the peer added to the authentication group.

In this example, the authentication group is named `auth_peer`, the peer that the group can authenticate is named `Server_net`, and the authentication group uses `123456` as the pre-shared key. In practice you should use a more secure pre-shared key.

```
config wanopt auth-group
   edit auth_peer
      set auth-method psk
      set psk 123456
      set peer-accept one
      set peer Server_net
   end
```

To add an authentication group that accepts WAN optimization connections from any peer - web-based manager

Add an authentication group that accepts any peer for situations where you do not have the **Peer Host IDs** or **IP Addresses** of the peers that you want to perform WAN optimization with. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP. An authentication group that accepts any peer is less secure than an authentication group that accepts defined peers or a single peer.

The example below sets the authentication method to **Pre-shared key**. You must add the same password to all FortiGate units using this authentication group.

1. Go to Wan Opt. & Cache > WAN Opt. Peer > Authentication Group.
2. Select **Create New** to add a new authentication group.
3. Configure the authentication group:

Name	Specify any name.
Authentication Method	Pre-shared key
Password	Enter a pre-shared key.
Peer Acceptance	Accept Any Peer

To add an authentication group that accepts WAN optimization connections from any peer - CLI:

In this example, the authentication group is named `auth_grp_1`. It uses a certificate named `WAN_Cert` and accepts any peer.

```
config wanopt auth-group
   edit auth_grp_1
      set auth-method cert
      set cert WAN_Cert
      set peer-accept any
   end
```

Secure tunneling

You can configure WAN optimization rules to use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel. WAN optimization uses FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. Peer-to-peer secure tunnels use the same TCP port as non-secure peer-to-peer tunnels (TCP port 7810).

To use secure tunneling, you must select **Enable Secure Tunnel** in a WAN optimization rule and add an authentication group. The authentication group specifies the certificate or pre-shared key used to set up the secure tunnel. The **Peer Acceptance** setting of the authentication group does not affect secure tunneling.

The FortiGate units at each end of the secure tunnel must have the same authentication group with the same name and the same configuration, including the same pre-shared key or certificate. To use certificates you must install the same certificate on both FortiGate units.

For active-passive WAN optimization you can select **Enable Secure Tunnel** only in the active rule. In peer-to-peer WAN optimization you select **Enable Secure Tunnel** in the WAN optimization rule on both FortiGate units.

For information about active-passive and peer-to-peer WAN optimization, see Manual (peer-to-peer) and active-passive WAN optimization on page 2828

For a secure tunneling configuration example, see Example Adding secure tunneling to an active-passive WAN optimization configuration on page 2866.

Monitoring WAN optimization peer performance

The WAN optimization peer monitor lists all of the WAN optimization peers that a FortiGate unit can perform WAN optimization with. These include peers manually added to the configuration as well as discovered peers.

The monitor lists each peer's name, IP address, and peer type. The peer type indicates whether the peer was manually added or discovered. To show WAN optimization performance, for each peer the monitor lists the percent of traffic reduced by the peer in client-side WAN optimization configurations and in server-side configurations (also called gateway configurations).

To view the peer monitor, go to **WAN Opt. & Cache > Monitor > Peer Monitor**.

Configuration examples

This chapter provides the basic examples to illustrate WAN optimization configurations introduced in the previous chapters.

Example Basic manual (peer-to-peer) WAN optimization configuration

In a manual (peer to peer) configuration the WAN optimization tunnel can be set up between one client-side FortiGate unit and one server-side FortiGate unit. The peer ID of the server-side FortiGate unit is added to the client-side WAN optimization policy. When the client-side FortiGate unit initiates a tunnel with the server-side FortiGate unit, the packets that initiate the tunnel include information that allows the server-side FortiGate unit to determine that it is a manual tunnel request. The server-side FortiGate unit does not require a WAN optimization profile; you just need to add the client peer host ID and IP address to the server-side FortiGate unit peer list and from the CLI an explicit proxy policy to accept WAN optimization tunnel connections.

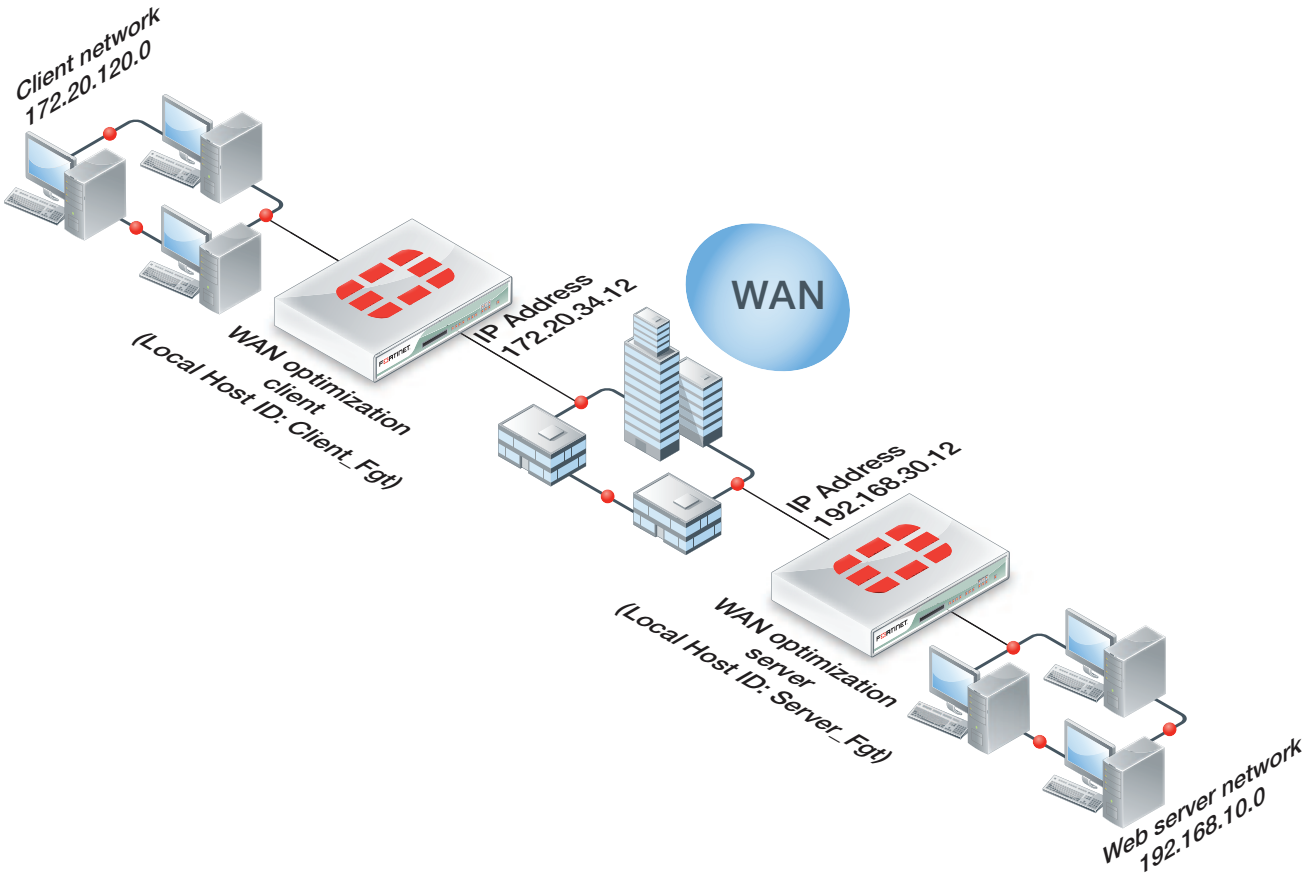
In a manual WAN optimization configuration, you create a manual WAN optimization security policy on the client-side FortiGate unit. To do this you must use the CLI to set `wanopt-detection` to `off` and to add the peer host ID of the server-side FortiGate unit to the WAN optimization security policy.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Peer-Fgt-1 with a WAN IP address of 172.20.34.12. This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Peer-Fgt-2 with a WAN IP address of 192.168.30.12. This unit is in front of a web server network with IP address 192.168.10.0.

This example customizes the default WAN optimization profile on the client-side FortiGate unit and adds it to the WAN optimization policy. You can also create a new WAN optimization profile.

Example manual (peer-to-peer) topology



General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit:
   - Add peers.
   - Configure the default WAN optimization profile to optimize HTTP traffic.
   - Add a manual WAN optimization security policy.
2. Configure the server-side FortiGate unit:
   - Add peers.
   - Add a WAN optimization tunnel policy.

Configuring basic peer-to-peer WAN optimization - web-based manager

Use the following steps to configure the example configuration from the web-based manager.

To configure the client-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the client-side FortiGate unit:

Local Host ID	Client-Fgt

2. Select **Apply**.
3. Select **Create New** and add the server-side FortiGate unit **Peer Host ID** and **IP Address** for the server-side FortiGate:

Peer Host ID	Server-Fgt
IP Address	192.168.30.12

4. Select **OK**.
5. Go to **Policy & Objects > Objects > Addresses** and select **Create New** to add a firewall address for the client network.

Category	Address
Name	Client-Net
Type	Subnet
Subnet / IP Range	172.20.120.0/24
Interface	port1

6. Select **Create New** to add a firewall address for the web server network.

Category	Address
Name	Web-Server-Net
Type	Subnet
Subnet / IP Range	192.168.10.0/24
Interface	port2

7. Go to **WAN Opt. & Cache > WAN Opt. Profiles > Profiles** and edit the default profile.
8. Select **Transparent Mode**.
9. Under Protocol, select **HTTP** and for HTTP select **Byte Caching**. Leave the HTTP **Port** set to 80.
10. Select **Apply** to save your changes.
11. Go to **Policy& Objects > Policy > IPv4** and add a WAN optimization security policy to the client-side FortiGate unit that accepts traffic to be optimized:

Incoming Interface	port1
Source Address	all
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

12. Select **Enable WAN Optimization** and configure the following settings:

Enable WAN Optimization	active
Profile	default

13. Select **OK**.
14. Edit the policy from the CLI to turn off `wanopt-detection`, add the peer ID of the server-side FortiGate unit, and the default WAN optimization profile. The following example assumes the ID of the policy is 5:

```
config firewall policy
  edit 5
    set wanopt-detection off
    set wanopt-peer Server-Fgt
    set wanopt-profile default
  end
```

When you set the detection mode to `off` the policy becomes a manual mode WAN optimization policy. On the web-based manager the WAN optimization part of the policy changes to the following:

Enable WAN Optimization	Manual (Profile: default, Peer: Peer-Fgt-2)

To configure the server-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the server-side FortiGate unit:

Local Host ID	Server-Fgt

2. Select **Apply**.
3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate unit:

Peer Host ID	Client-Fgt
IP Address	172.20.34.12

4. Select **OK**.
5. Enter the following CLI command to add an explicit proxy policy to accept WAN optimization tunnel connections.

```
configure firewall explicit-proxy-policy
```

```
    edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
    next
end
```

Configuring basic peer-to-peer WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit

1. Add the Local Host ID to the client-side FortiGate configuration:

```
config wanopt settings
  set host-id Client-Fgt
end
```

2. Add the server-side Local Host ID to the client-side peer list:

```
config wanopt peer
  edit Server-Fgt
  set ip 192.168.30.12
end
```

3. Add a firewall address for the client network.

```
config firewall address
  edit Client-Net
    set type ipmask
    set subnet 172.20.120.0 255.255.255.0
    set associated-interface port1
  end
```

4. Add a firewall address for the web server network.

```
config firewall address
  edit Web-Server-Net
    set type ipmask
    set subnet 192.168.10.0 255.255.255.0
    set associated-interface port2
  end
```

5. Edit the default WAN optimization profile, select transparent mode, enable HTTP WAN optimization and enable byte caching for HTTP. Leave the HTTP Port set to 80.

```
config wanopt profile
  edit default
    set transparent enable
      config http
        set status enable
        set byte-caching enable
      end
  end
```

6. Add a WAN optimization security policy to the client-side FortiGate unit to accept the traffic to be optimized:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr all
      set dstaddr all
      set action accept
      set service ALL
      set schedule always
      set wanopt enable
      set wanopt-profile default
      set wanopt-detection off
      set wanopt-peer Server-Fgt
   end
```

To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:

```
config wanopt settings
   set host-id Server-Fgt
end
```

2. Add the client-side Local Host ID to the server-side peer list:

```
config wanopt peer
   edit Client-Fgt
   set ip 192.168.30.12
end
```

3. Add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
end
```

Testing and troubleshooting the configuration

To test the configuration attempt to start a web browsing session between the client network and the web server network. For example, from a PC on the client network browse to the IP address of a web server on the web server network, for example http://192.168.10.100. Even though this address is not on the client network you should be able to connect to this web server over the WAN optimization tunnel.

If you can connect, check WAN optimization monitoring (go to **WAN Opt. & Cache > Monitor > Monitor**). If WAN optimization has been forwarding the traffic the WAN optimization monitor should show the protocol that has been optimized (in this case HTTP) and the reduction rate in WAN bandwidth usage.

If you can't connect you can try the following to diagnose the problem:

- Review your configuration and make sure all details such as address ranges, peer names, and IP addresses are correct.
- Confirm that the security policy on the client-side FortiGate unit is accepting traffic for the 192.168.10.0 network. You can do this by checking the policy monitor (**Policy & Objects > Monitor > Policy Monitor**). Look for sessions that use the policy ID of this policy.
- Check routing on the FortiGate units and on the client and web server networks to make sure packets can be forwarded as required. The FortiGate units must be able to communicate with each other, routing on the client network must allow packets destined for the web server network to be received by the client-side FortiGate unit, and packets from the server-side FortiGate unit must be able to reach the web servers.

You can use the following `get` and `diagnose` commands to display information about how WAN optimization is operating.

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output for the client-side FortiGate unit shows 10 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to off).

```
diagnose wad tunnel list

Tunnel: id=100 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=100 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=348 bytes_out=384

Tunnel: id=99 type=manual
vd=0 shared=no uses=0 state=3
peer name=Web-servers id=99 ip=192.168.30.12
SSL-secured-tunnel=no auth-grp=
bytes_in=348 bytes_out=384

Tunnel: id=98 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=98 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=348 bytes_out=384

Tunnel: id=39 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=39 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1068 bytes_out=1104

Tunnel: id=7 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=7 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=8 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=8 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=5 type=manual
```

```
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=5 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=4 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=4 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=1 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=1 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=2 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web-servers id=2 ip=192.168.30.12
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnels total=10 manual=10 auto=0
```

Example Active-passive WAN optimization

In active-passive WAN optimization you add an active WAN optimization policy to the client-side FortiGate unit and you add a WAN optimization tunnel policy and a passive WAN optimization policy to the server-side FortiGate unit.

The active policy accepts the traffic to be optimized and sends it down the WAN optimization tunnel to the server-side FortiGate unit. The active policy can also apply security profiles and other features to traffic before it exits the client-side FortiGate unit.

A tunnel explicit proxy policy on the sever-side FortiGate unit allows the server-side FortiGate unit to form a WAN optimization tunnel with the client-side FortiGate unit. The passive WAN optimization policy is required because of the active policy on the client-side FortiGate unit. You can also use the passive policy to apply WAN optimization transparent mode and features such as security profiles, logging, traffic shaping and web caching to the traffic before it exits the server-side FortiGate unit.

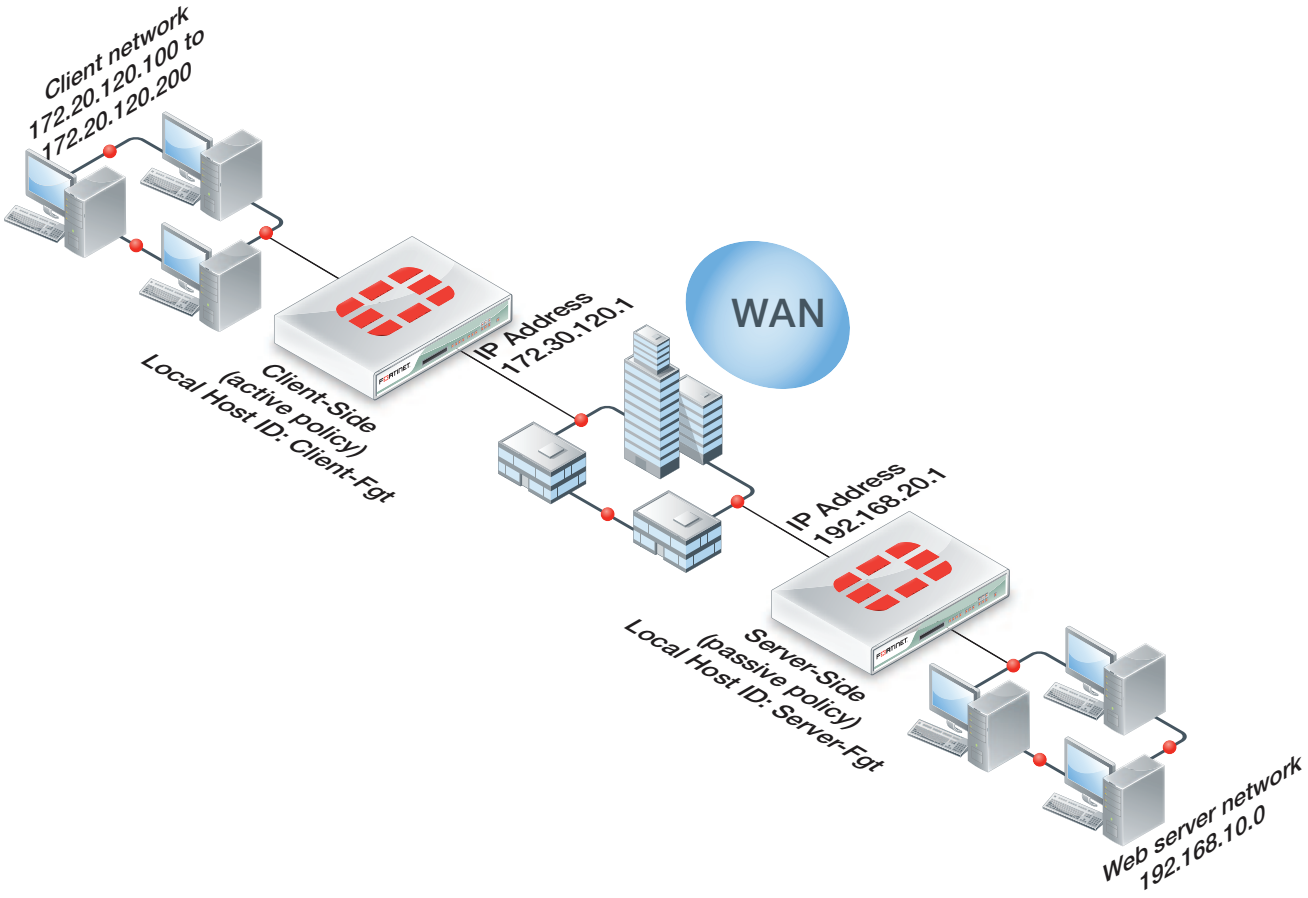
Network topology and assumptions

On the client-side FortiGate unit this example configuration includes a WAN optimization profile that optimizes CIFS, HTTP, and FTP traffic and an active WAN optimization policy. The active policy also applies virus scanning to the WAN optimization traffic.

On the server-side FortiGate unit, the passive policy applies application control to the WAN optimization traffic.

In this example, WAN optimization transparent mode is selected in the WAN optimization profile and the passive WAN optimization policy accepts this transparent mode setting. This means that the optimized packets maintain their original source and destination addresses. As a result, routing on the client network must be configured to route packets for the server network to the client-side FortiGate unit. Also the routing configuration on the server network must be able to route packets for the client network to the server-side FortiGate unit.

Example active-passive WAN optimization topology



General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit:
   - Add peers.
   - Add a WAN optimization profile to optimize CIFS, FTP, and HTTP traffic.
   - Add firewall addresses for the client and web server networks.
   - Add an active WAN optimization policy.
2. Configure the server-side FortiGate unit by:
   - Add peers.
   - Add firewall addresses for the client and web server networks.
   - Add a passive WAN optimization policy.
   - Add a WAN optimization tunnel policy.

Configuring basic active-passive WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager.

To configure the client-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the client-side FortiGate unit:

Local Host ID	Client-Fgt

2. Select **Apply**.
3. Select **Create New** and add a Peer Host ID and the **IP Address** for the server-side FortiGate unit:

Peer Host ID	Server-Fgt
IP Address	192.168.20.1

4. Select **OK**.
5. Go to **WAN Opt. & Cache > WAN Opt. Profiles > Profiles** and select Create New to add a WAN optimization profile to optimize CIFS, HTTP, and FTP traffic:

Name	Custom-wan-opt-pro
Transparent Mode	Select

6. Select the **CIFS** protocol, select **Byte Caching** and set the **Port** to 445.
7. Select the **FTP** protocol, select **Byte Caching** and set the **Port** to 21.
8. Select the **HTTP** protocol, select **Byte Caching** and set the **Port** to 80.
9. Select **OK**.
10. Go to **Policy & Objects > Objects > Addresses** and select **Create New** to add an address for the client network.

Category	Address
Address Name	Client-Net
Type	IP Range
Subnet / IP Range	172.20.120.100-172.20.120.200
Interface	port1

11. Select **Create New** to add an address for the web server network.

Category	Address

Address Name	Web-Server-Net
Type	Subnet
Subnet / IP Range	192.168.10.0/24
Interface	port2

12. Go to **Policy & Objects > Policy > IPv4** and select **Create New** to add an active WAN optimization security policy:

Incoming Interface	port1
Source Address	Client-Net
Outgoing Interface	port2
Destination Address	Web-Server-Net
Schedule	always
Service	HTTP FTP SMB
Action	ACCEPT

13. Turn on **WAN Optimization** and configure the following settings:

WAN Optimization	active
Profile	Custom-wan-opt-pro

14. Turn on Antivirus and select the **default** antivirus profile.
15. Select **OK**.

To configure the server-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the server-side FortiGate unit:

Local Host ID	Server-Fgt

2. Select **Apply**.
3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate unit:

Peer Host ID	Client-Fgt
IP Address	172.30.120.1

4. Select **OK**.
5. Go to **Policy & Objects > Objects > Addresses** and select **Create New** to add an address for the client network.

Category	Address
Address Name	Client-Net
Type	IP Range
Subnet / IP Range	172.20.120.100-172.20.120.200
Interface	port1

6. Select **Create New** to add a firewall address for the web server network.

Category	Address
Address Name	Web-Server-Net
Type	Subnet
Subnet / IP Range	192.168.10.0/24
Interface	port2

7. Select **OK**.
8. Select **Policy & Objects > Policy > IPv4** and select **Create New** to add a passive WAN optimization policy that applies application control.

Incoming Interface	port2
Source Address	Client-Net
Outgoing Interface	port1
Destination Address	Web-Server-Net
Schedule	always
Service	ALL
Action	ACCEPT

9. Turn on **WAN Optimization** and configure the following settings:

WAN Optimization	passive
Passive Option	default

10. Select **OK**.
11. From the CLI enter the following command to add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy
```

```
    edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
    next
end
```

Configuring basic active-passive WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit

1. Add the Local Host ID to the client-side FortiGate configuration:

```
config wanopt settings
  set host-id Client-Fgt
end
```

2. Add the server-side Local Host ID to the client-side peer list:

```
config wanopt peer
  edit Server-Fgt
  set ip 192.168.20.1
end
```

3. Add a WAN optimization profile to optimize CIFS, HTTP, and FTP traffic.

```
config wanopt profile
  edit Custom-wan-opt-pro
    config cifs
      set status enable
      set byte-caching enable
      set port 445
    end
    config http
      set status enable
      set byte-caching enable
      set port 80
    end
    config ftp
      set status enable
      set byte-caching enable
      set port 21
    end
  end
```

4. Add a firewall address for the client network.

```
config firewall address
  edit Client-Net
    set type iprange
    set start-ip 172.20.120.100
    set end-ip 172.20.120.200
    set associated-interface port1
  end
```

5. Add a firewall address for the web server network.

```
config firewall address
   edit Web-Server-Net
      set type ipmask
      set subnet 192.168.10.0 255.255.255.0
      set associated-interface port2
   end
```

6. Add an active WAN optimization security policy that applies virus scanning:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Client-net
      set dstaddr Web-Server-Net
      set action accept
      set service HTTP FTP SMB
      set schedule always
      set wanopt enable
      set wanopt-detection active
      set wanopt-profile Custom-wan-opt-pro
   end
```

To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:

```
config wanopt settings
   set host-id Server-Fgt
end
```

2. Add the client-side Local Host ID to the server-side peer list:

```
config wanopt peer
   edit Client-Fgt
   set ip 172.20.120.1
end
```

3. Add a firewall address for the client network.

```
config firewall address
   edit Client-Net
      set type iprange
      set start-ip 172.20.120.100
      set end-ip 172.20.120.200
      set associated-interface port1
   end
```

4. Add a firewall address for the web server network.

```
config firewall address
   edit Web-Server-Net
      set type ipmask
      set subnet 192.168.10.0 255.255.255.0
      set associated-interface port2
   end
```

5. Add a passive WAN optimization policy.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Client-Net
      set dstaddr Web-Server-Net
      set action accept
```

```
      set service ALL
      set schedule always
      set wanopt enable
      set wanopt-detection passive
      set wanopt-passive-opt default
    end
```

6. Add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
end
```

Testing and troubleshooting the configuration

To test the configuration attempt to start a web browsing session between the client network and the web server network. For example, from a PC on the client network browse to the IP address of a web server on the web server network, for example http://192.168.10.100. Even though this address is not on the client network you should be able to connect to this web server over the WAN optimization tunnel.

If you can connect, check WAN optimization monitoring (go to **WAN Opt. & Cache > Monitor > Monitor**). If WAN optimization has been forwarding the traffic the WAN optimization monitor should show the protocol that has been optimized (in this case HTTP) and the reduction rate in WAN bandwidth usage.

If you can't connect you can try the following to diagnose the problem:

- Review your configuration and make sure all details such as address ranges, peer names, and IP addresses are correct.
- Confirm that the security policy on the Client-Side FortiGate unit is accepting traffic for the 192.168.10.0 network and that this security policy does not include security profiles. You can do this by checking the FortiGate session table from the dashboard. Look for sessions that use the policy ID of this policy.
- Check routing on the FortiGate units and on the client and web server networks to make sure packets can be forwarded as required. The FortiGate units must be able to communicate with each other, routing on the client network must allow packets destined for the web server network to be received by the client-side FortiGate unit, and packets from the server-side FortiGate unit must be able to reach the web servers etc.

You can use the following `get` and `diagnose` commands to display information about how WAN optimization is operating

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output shows 3 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to on).

```
diagnose wad tunnel list

Tunnel: id=139 type=auto
   vd=0 shared=no uses=0 state=1
   peer name= id=0 ip=unknown
   SSL-secured-tunnel=no auth-grp=test
```

```
   bytes_in=744 bytes_out=76

Tunnel: id=141 type=auto
   vd=0 shared=no uses=0 state=1
   peer name= id=0 ip=unknown
   SSL-secured-tunnel=no auth-grp=test
   bytes_in=727 bytes_out=76

Tunnel: id=142 type=auto
   vd=0 shared=no uses=0 state=1
   peer name= id=0 ip=unknown
   SSL-secured-tunnel=no auth-grp=test
   bytes_in=727 bytes_out=76

Tunnels total=3 manual=0 auto=3
```

Example Adding secure tunneling to an active-passive WAN optimization configuration

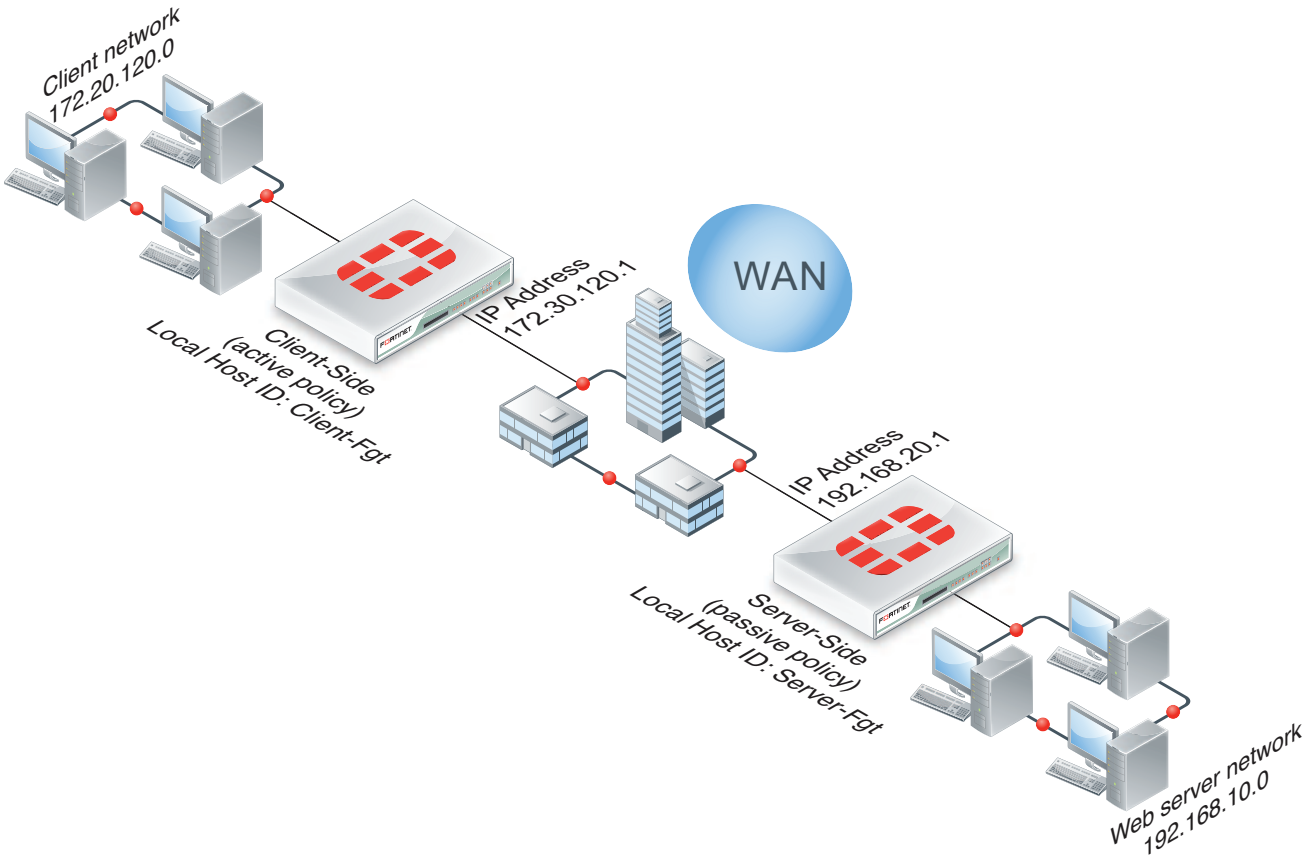
This example shows how to configure two FortiGate units for active-passive WAN optimization with secure tunneling. The same authentication group is added to both FortiGate units. The authentication group includes a password (or pre-shared key) and has **Peer Acceptance** set to **Accept any Peer**. An active policy is added to the client-side FortiGate unit and a passive policy to the server-side FortiGate unit. The active policy includes a profile that performs secure tunneling, optimizes HTTP traffic, and uses Transparent Mode and byte caching.

The authentication group is named **Auth-Secure-Tunnel** and the password for the pre-shared key is **2345678**. The topology for this example is shown below. This example includes web-based manager configuration steps followed by equivalent CLI configuration steps. For information about secure tunneling, see Secure tunneling on page 2849.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Client-net with a WAN IP address of 172.30.120.1.This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Web-servers and has a WAN IP address of 192.168.20.1. This unit is in front of a web server network with IP address 192.168.10.0.

Example active-passive WAN optimization and secure tunneling topology



General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit:
   - Add peers.
   - Add an authentication group.
   - Add an active WAN optimization policy.
2. Configure the server-side FortiGate unit.
   - Add peers.
   - Add the same authentication group
   - Add a passive WAN optimization policy that applies application control.
   - Add a WAN optimization tunnel policy.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring WAN optimization with secure tunneling - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure the client-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the client-side FortiGate unit:

Local Host ID	Client-Fgt

2. Select **Apply** to save your setting.
3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the server-side FortiGate unit:

Peer Host ID	Server-Fgt
IP Address	192.168.20.1

4. Select **OK**.
5. Go to **Wan Opt. & Cache > WAN Opt. Peers > Authentication Groups** and select **Create New** to add the authentication group to be used for secure tunneling:

Name	Auth-Secure-Tunnel
Authentication Method	Pre-shared key
Password	2345678
Peer Acceptance	Accept Any Peer

6. Select **OK**.
7. Go to **Wan Opt. & Cache > WAN Opt. Profiles > Profiles** and select **Create New** to add a WAN optimization profile that enables secure tunneling and includes the authentication group:

Name	Secure-wan-op-pro
Transparent Mode	Select
Authentication Group	Auth-Secure-tunnel

8. Select the **HTTP** protocol, select Secure Tunneling and **Byte Caching** and set the **Port** to 80.
9. Select **OK**.
10. Go to Policy & **Objects > Objects > Addresses** and select **Create New** to add a firewall address for the client network.

Category	Address

Name	Client-Net
Type	Subnet
Subnet / IP Range	172.20.120.0/24
Interface	port1

11. Select **Create New** to add a firewall address for the web server network.

Category	Address
Address Name	Web-Server-Net
Type	Subnet
Subnet / IP Range	192.168.10.0/24
Interface	port2

12. Go to **Policy & Objects > Policy > IPv4** and select **Create New** to add an active WAN optimization security policy:

Incoming Interface	port1
Source Address	Client-Net
Outgoing Interface	port2
Destination Address	Web-Server-Net
Schedule	always
Service	HTTP
Action	ACCEPT

13. Turn on **WAN Optimization** and configure the following settings:

WAN Optimization	active
Profile	Secure-wan-opt-pro

14. Select **OK**.

To configure the server-side FortiGate unit

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Peers** and enter a **Local Host ID** for the server-side FortiGate unit:

Local Host ID	Server-Fgt

2. Select **Apply** to save your setting.
3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate unit:

Peer Host ID	Client-Fgt
IP Address	172.30.120.1

4. Select **OK**.
5. Go to **Wan Opt. & Cache > WAN Opt. Peers > Authentication Groups** and select **Create New** and add an authentication group to be used for secure tunneling:

Name	Auth-Secure-Tunnel
Authentication Method	Pre-shared key
Password	2345678
Peer Acceptance	Accept Any Peer

6. Select **OK**.
7. Go to **Policy & Objects > Objects > Addresses** and select **Create New** to add a firewall address for the client network.

Category	Address
Name	Client-Net
Type	Subnet
Subnet / IP Range	172.20.120.0/24
Interface	port1

8. Select **Create New** to add a firewall address for the web server network.

Category	Address
Address Name	Web-Server-Net
Type	Subnet
Subnet / IP Range	192.168.10.0/24
Interface	port2

9. Select **OK**.
10. Select **Create New** to add a passive WAN optimization policy that applies application control.

Incoming Interface	port2

Source Address	Client-Net
Outgoing Interface	port1
Destination Address	Web-Server-Net
Schedule	always
Service	ALL
Action	ACCEPT

11. Turn on **WAN Optimization** and configure the following settings:

WAN Optimization	passive
Passive Option	default

12. Select **OK**.
13. From the CLI enter the following command to add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
end
```

Configuring WAN optimization with secure tunneling - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To the client-side FortiGate unit

1. Add the Local Host ID to the client-side FortiGate configuration:

```
config wanopt settings
   set host-id Client-Fgt
end
```

2. Add the server-side Local Host ID to the client-side peer list:

```
config wanopt peer
   edit Server-Fgt
   set ip 192.168.20.1
end
```

3. Add a new authentication group to be used for secure tunneling:

```
config wanopt auth-group
   edit Auth-Secure-Tunnel
      set auth-method psk
```

```
      set psk 2345678
   end
```

Leave `peer-accept` at its default value.

4. Add a WAN optimization profile that enables secure tunneling and includes the authentication group, enables HTTP protocol optimization, and enables secure tunneling and byte caching for HTTP traffic:

```
config wanopt profile
   edit Secure-wan-op-pro
      set auth-group Auth-Secure-Tunnel
      config http
         set status enable
         set secure-tunnel enable
         set byte-caching enable
         set port 80
      end
   end
```

5. Add a firewall address for the client network.

```
config firewall address
   edit Client-Net
      set type ipmask
      set subnet 172.20.120.0 255.255.255.0
      set associated-interface port1
   end
```

6. Add a firewall address for the web server network.

```
config firewall address
   edit Web-Server-Net
      set type ipmask
      set subnet 192.168.10.0 255.255.255.0
      set associated-interface port2
   end
```

7. Add an active WAN optimization security policy that includes the WAN optimization profile that enables secure tunneling and that applies virus scanning:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Client-Net
      set dstaddr Web-Server-Net
      set action accept
      set service HTTP
      set schedule always
      set wanopt enable
      set wanopt-detection active
      set wanopt-profile Secure-wan-opt-pro
   end
```

To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:

```
config wanopt settings
   set host-id Server-Fgt
end
```

2. Add the client-side Local Host ID to the server-side peer list:

```
config wanopt peer
   edit Client-Fgt
   set ip 172.20.120.1
end
```

3. Add an authentication group to be used for secure tunneling:

```
config wanopt auth-group
   edit Auth-Secure-Tunnel
      set auth-method psk
      set psk 2345678
   end
```

   Leave `peer-accept` at its default value.

4. Add a firewall address for the client network.

```
config firewall address
   edit Client-Net
      set type ipmask
      set subnet 172.20.120.0 255.255.255.0
      set associated-interface port1
   end
```

5. Add a firewall address for the web server network.

```
config firewall address
   edit Web-Server-Net
      set type ipmask
      set subnet 192.168.10.0 255.255.255.0
      set associated-interface port2
   end
```

6. Add a passive WAN optimization policy.

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr Client-Net
      set dstaddr Web-Server-Net
      set action accept
      set service ALL
      set schedule always
      set wanopt enable
      set wanopt-detection passive
      set wanopt-passive-opt default
   end
```

7. Add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
```

```
    next
  end
```

Web caching and SSL offloading

FortiGate web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Web caching supports caching of HTTP 1.0 and HTTP 1.1 web sites. See RFC 2616 for information about web caching for HTTP 1.1.

Web caching supports caching of Flash content over HTTP but does not cache audio and video streams including Flash videos and streaming content that use native streaming protocols such as RTMP.

The first time a file is received by web caching it is cached in the format it is received in, whether it be compressed or uncompressed. When the same file is requested by a client but in a different compression format, the cached file is converted to the new compressed format before being sent to the client.

There are three significant advantages to using web caching to improve HTTP and WAN performance:

- reduced bandwidth consumption because fewer requests and responses go over the WAN or Internet.
- reduced web server load because there are fewer requests for web servers to handle.
- reduced latency because responses for cached requests are available from a local FortiGate unit instead of from across the WAN or Internet.

You can use web caching to cache any web traffic that passes through the FortiGate unit, including web pages from web servers on a LAN, WAN or on the Internet. You apply web caching by enabling the web caching option in any security policy. When enabled in a security policy, web caching is applied to all HTTP sessions accepted by the security policy. If the security policy is an explicit web proxy security policy, the FortiGate unit caches explicit web proxy sessions.

Turning on web caching for HTTP and HTTPS traffic

Web caching can be applied to any HTTP or HTTPS traffic by enabling web caching in a security policy that accepts the traffic. This includes IPv4, IPv6, WAN optimization and explicit web proxy traffic. Web caching caches all HTTP traffic accepted by a policy on TCP port 80.

You can add web caching to a policy to:

- Cache Internet HTTP traffic for users on an internal network to reduce Internet bandwidth use. Do this by selecting the web cache option for security policies that allow users on the internal network to browse web sites on the Internet.
- Reduce the load on a public facing web server by caching objects on the FortiGate unit. This is a reverse proxy with web caching configuration. Do this by selecting the web cache option for a security policy that allows users on the Internet to connect to the web server.
- Cache outgoing explicit web proxy traffic when the explicit proxy is used to proxy users in an internal network who are connecting to the web servers on the Internet. Do this by selecting the web cache option for explicit web proxy security policies that allow users on the internal network to browse web sites on the Internet.
- Combine web caching with WAN optimization. You can enable web caching in any WAN optimization security policy. This includes manual, active, and passive WAN optimization policies and WAN optimization tunnel policies. You can enable web caching on both the client-side and the server-side FortiGate units or on just one or the other.

For optimum performance you can enable web caching on both the client-side and server-side FortiGate units. In this way only uncached content is transmitted through the WAN optimization tunnel. All cached content is access locally by clients from the client side FortiGate unit.

One important use for web caching is to cache software updates (for example, Windows Updates or iOS updates. When updates occur a large number of users may all be trying to download these updates at the same time. Caching these updates will be a major performance improvement and also have a potentially large impact on reducing Internet bandwidth use. You may want to adjust the maximum cache object size to make sure these updates are cached. SeeMax cache object size on page 2880.

Turning on web caching for HTTPS traffic

Web caching can also cache the content of HTTPS traffic on TCP port 443. With HTTPS web caching, the FortiGate unit receives the HTTPS traffic on behalf of the client, opens up the encrypted traffic and extracts content to be cached. Then FortiGate unit re-encrypts the traffic and sends it on to its intended recipient. It is very similar to a man-in-the-middle attack.

You enable HTTPS web caching from the CLI in a security policy or an explicit proxy policy that accepts the traffic to be cached using `webcache-https`. For a firewall policy:

```
config firewall policy
   edit 0
      .
      .
      .
      set webcache enable
      set webcache-https any
      .
      .
      .
   end
```

For an explicit web proxy policy:

```
config firewall policy
   edit 0
      set proxy web
      .
      .
      .
      set webcache enable
      set webcache-https any
      .
      .
      .
   end
```

Web caching for HTTPS traffic is not supported if WAN optimization is enabled.

The `any` setting causes the FortiGate unit to re-encrypt the traffic with the FortiGate unit's certificate rather than the original certificate. This configuration can cause errors for HTTPS clients because the name on the certificate does not match the name on the web site.

You can stop these errors from happening by configuring HTTPS web caching to use the web server's certificate by setting `webcache-https` to `ssl-server`. This option is available for both firewall policies and explicit web proxy policies.

```
config firewall policy
   edit 0
      .
      .
      .
      set webcache enable
      set webcache-https ssl-server
      .
      .
      .
   end
```

The `ssl-server` option causes the FortiGate unit to re-encrypt the traffic with a certificate that you imported into the FortiGate unit. You can add certificates using the following command:

```
config firewall ssl-server
   edit corporate-server
      set ip <Web-Server-IP>
      set port 443
      set ssl-mode { full | half}
      set ssl-cert <Web-Server-Cert>
   end
```

Where:

`Web-Server-IP` is the web server's IP address.

`Web-Server-Cert` is a web server certificate imported into the FortiGate unit.

The SSL server configuration also determines whether the SSL server is operating in half or full mode and the port used for the HTTPS traffic.

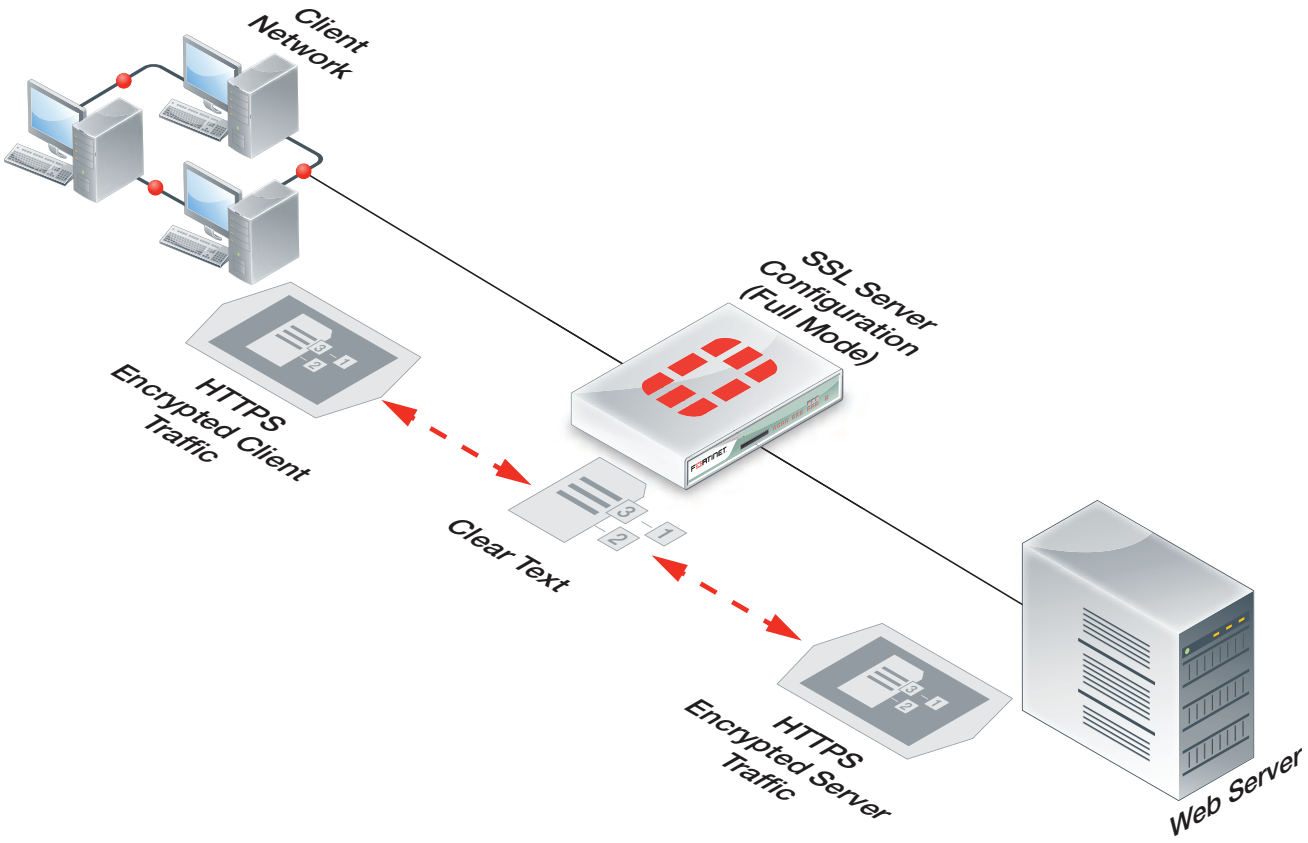
You can add multiple SSL server certificates in this way. When web caching processing an SSL stream if it can find a certificate that matches the web server IP address and port of one of the added SSL servers; that certificate is used to encrypt the SSL traffic before sending it to the client. As a result the client does not generate SSL certificate errors.

Web caching uses the FortiGate unit's FortiASIC to accelerate SSL decryption/encryption performance.

Full mode SSL server configuration

The `ssl-mode` option determines whether the SSL server operates in half or full mode. In full mode the FortiGate unit performs both decryption and encryption of the HTTPS traffic. The full mode sequence is shown below.

Full mode SSL server configuration



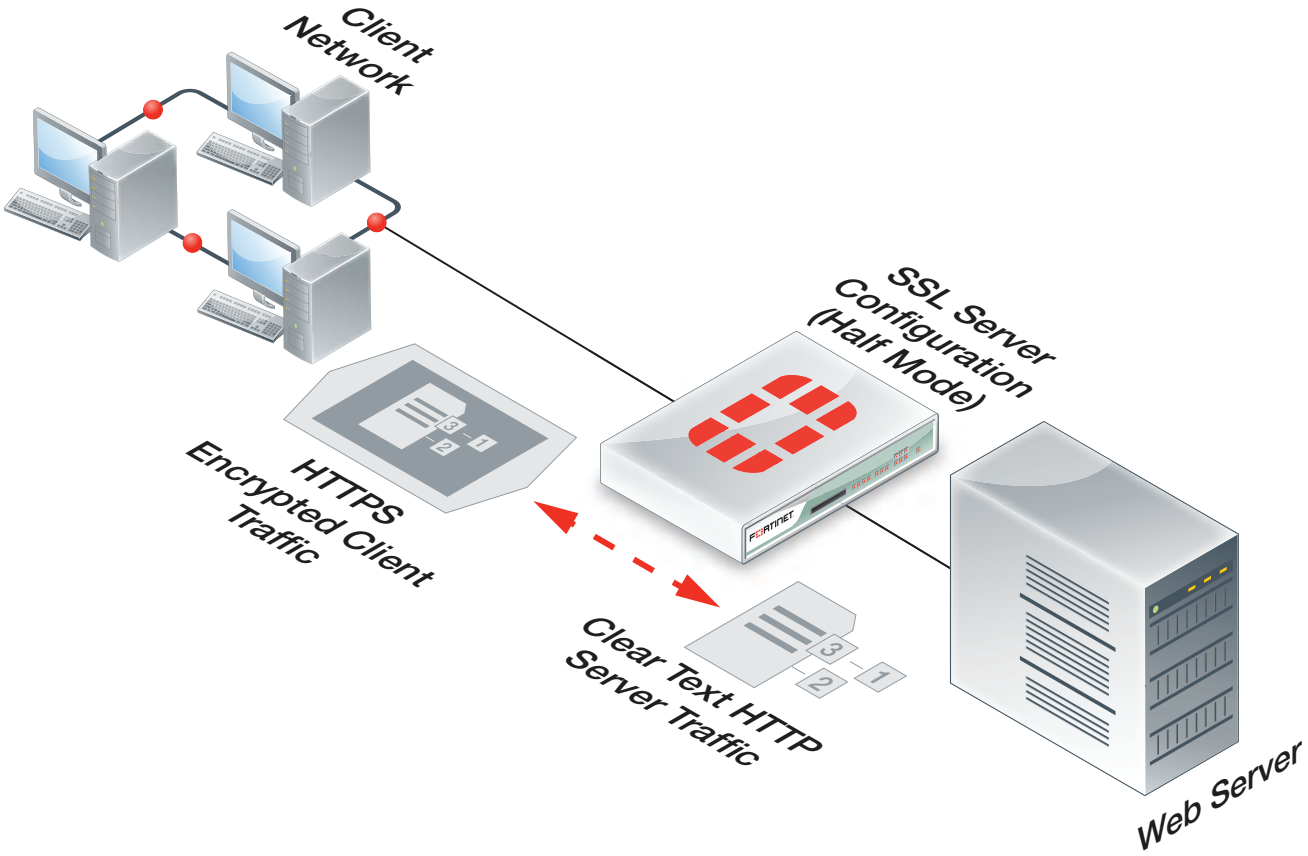
In full mode the FortiGate unit is acting as a man in the middle, decrypting and encrypting the traffic. So both the client and the web server see encrypted packets.

Usually the port of the encrypted HTTPS traffic is always 443. However, in the SSL server configuration you can set the port used for HTTPS traffic. This port is not altered by the SSL Server. So for example, if the SSL Server receives HTTPS traffic on port 443, the re-encrypted traffic forwarded to the FortiGate unit to the server or client will still use port 443.

Half mode SSL server configuration

In half mode, the FortiGate unit only performs one encryption or decryption action. If HTTP packets are received, the half mode SSL server encrypts them and converts them to HTTPS packets. If HTTPS packets are received, the SSL server decrypts them and converts them to HTTP packets.

Half mode SSL server configuration



In half mode, the FortiGate unit is acting like an SSL accelerator, offloading HTTPS decryption from the web server to the FortiGate unit. Since FortiGate units can accelerate SSL processing, the end result could be improved web site performance.

Usually the port of the encrypted traffic is always 443. However, in the SSL server configuration you can set the port used for HTTPS traffic. No matter what port is used for the HTTPS traffic, the decrypted HTTP traffic uses port 80.

Changing the ports on which to look for HTTP and HTTPS traffic to cache

By default FortiOS assumes HTTP traffic uses TCP port 80 and HTTPS traffic uses port 443. So web caching caches all HTTP traffic accepted by a policy on TCP port 80 and all HTTPS traffic on TCP port 443. If you want to cache HTTP or HTTPS traffic on other ports, you can enable security profiles for the security policy and configure a proxy options profile to that looks for HTTP and HTTPS traffic on other TCP ports. To configure a proxy options profile go to **Policy & Options > Policy > Proxy Options**.

Setting the HTTP port to **Any** in a proxy options profile is not compatible with web caching. If you set the HTTP port to any, web caching only caches HTTP traffic on port 80.

Web caching and HA

You can configure web caching on a FortiGate HA cluster. The recommended best practice HA configuration for web caching is active-passive mode. When the cluster is operating, all web caching sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance web caching sessions.

In a cluster, only the primary unit stores the web cache database. The databases is not synchronized to the subordinate units. So, after a failover, the new primary unit must build its web cache.

Web caching and memory usage

To accelerate and optimize disk access and to provide better throughput and less latency, web caching uses provisioned memory to reduce disk I/O and increase disk I/O efficiency. In addition, web caching requires a small amount of additional memory per session for comprehensive flow control logic and efficient traffic forwarding.

When web caching is enabled you will see a reduction in available memory. The reduction increases when more web caching sessions are being processed. If you are thinking of enabling web caching on an operating FortiGate unit, make sure its memory usage is not maxed out during high traffic periods.

In addition to using the system dashboard to see the current memory usage you can use the `get test wad 2` command to see how much memory is currently being used by web caching. See get test {wad | wccpd} <test_level> on page 2947 for more information.

Changing web cache settings

In most cases, the default settings for the WAN optimization web cache are acceptable. However, you may want to change them to improve performance or optimize the cache for your configuration. To change these settings, go to **WAN Opt. & Cache > Cache > Settings.**

From the FortiGate CLI, you can use the `config wanopt webcache` command to change these WAN optimization web cache settings.

For more information about many of these web cache settings, see RFC 2616.

Always revalidate

Select to always revalidate requested cached objects with content on the server before serving them to the client.

Max cache object size

Set the maximum size of objects (files) that are cached. The default size is 512000 KB and the range is 1 to 4294967 KB. This setting determines the maximum object size to store in the web cache. Objects that are larger than this size are still delivered to the client but are not stored in the FortiGate web cache.

For most web traffic the default maximum cache object size is recommended. However, since web caching can also cache larger objects such as Windows updates, Mac OS updates, iOS updates or other updates delivered using HTTP you might want to increase the object size to make sure these updates are cached. Caching these

updates can save a lot of Internet bandwidth and improve performance when major updates are released by these vendors.

Negative response duration

Set how long in minutes that the FortiGate unit caches error responses from web servers. If error responses are cached, then subsequent requests to the web cache from users will receive the error responses regardless of the actual object status.

The default is 0, meaning error responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes.

Fresh factor

Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100%. For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the **Fresh Factor** the less often the checks occur.

For example, if you set the **Max TTL** value and **Default TTL** to 7200 minutes (5 days) and set the **Fresh Factor** to 20, the web cache check the cached objects 5 times before they expire, but if you set the **Fresh Factor** to 100, the web cache will check once.

Max TTL

The maximum amount of time (Time to Live) an object can stay in the web cache without the cache checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days) and the range is 1 to 5256000 minutes (5256000 minutes in a year).

Min TTL

The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. The default is 5 minutes and the range is 1 to 5256000 minutes (5256000 minutes in a year).

Default TTL

The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours) and the range is 1 to 5256000 minutes (5256000 minutes in a year).

Proxy FQDN

The fully qualified domain name (FQDN) for the proxy server. This is the domain name to enter into browsers to access the proxy server. This field is for information only can be changed from the explicit web proxy configuration.

Max HTTP request length

The maximum length of an HTTP request that can be cached. Larger requests will be rejected. This field is for information only can be changed from the explicit web proxy configuration.

Max HTTP message length

The maximum length of an HTTP message that can be cached. Larger messages will be rejected. This field is for information only can be changed from the explicit web proxy configuration.

Ignore

Select the following options to ignore some web caching features.

If-modified-since	By default, if the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object. Enable ignoring if-modified-since to override this behavior.
HTTP 1.1 conditionals	HTTP 1.1 provides additional controls to the client over the behavior of caches toward stale objects. Depending on various cache-control headers, the FortiGate unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616.Enable ignoring HTTP 1.1 Conditionals to override this behavior.
Pragma-no-cache	Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This means that the FortiGate unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh.Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if you enable ignoring Pragma-no-cache, then the PNC header from the client request is ignored. The FortiGate unit treats the request as if the PNC header is not present.
IE Reload	Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select **Refresh**. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object. Enable ignoring IE reload to cause the FortiGate unit to ignore the PNC interpretation of the Accept / header.

Cache Expired Objects

Applies only to type-1 objects. When this option is selected, expired type-1 objects are cached (if all other conditions make the object cacheable).

Revalidated Pragma-no-cache

The pragma-no-cache (PNC) header in a client's request can affect how efficiently the FortiGate unit uses bandwidth. If you do not want to completely ignore PNC in client requests (which you can do by selecting to ignore Pragma-no-cache, above), you can nonetheless lower the impact on bandwidth usage by selecting **Revalidate Pragma-no-cache**.

When you select **Revalidate Pragma-no-cache**, a client's non-conditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the 304 Not Modified response, which consumes less server-side bandwidth, because the OCS has not been forced to otherwise return full content.

By default, **Revalidate Pragma-no-cache** is disabled and is not affected by changes in the top-level profile.

Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, you should also configure byte-range support when you configure the **Revalidate pragma-no-cache** option.

Forwarding URLs to forwarding servers and exempting web sites from web caching

You can go to **System > Network > Explicit Proxy** and use the URL match list to forward URL patterns to forwarding servers and create a list of URLs that are exempt from web caching.

Forwarding URLs and URL patterns to forwarding servers

As part of configuring the explicit web proxy you can configure proxy chaining by adding web proxy forwarding servers. See "Proxy chaining (web proxy forwarding servers) ".

You can then use the URL match list to always forward explicit web proxy traffic destined for configured URLs or URL patterns to one of these forwarding servers. For example, you might want to forward all traffic for a specific country to a proxy server located in that country.

To forward traffic destined for a URL to a forwarding server that you have already added, go to **System > Network > Explicit Proxy** and select **Create New**. Add a name for the URL match entry and enter the URL or URL pattern. You can use wildcards such as * and ? and you can use a numeric IP address. Select **Forward to Server** and select a web proxy forwarding server from the list.

You can also exempt the URL or URL pattern from web caching.

Use the following command to forward all .ca traffic to a proxy server and all .com traffic to another proxy server.

```
config web-proxy url-match
   edit "com"
      set forward-server "server-commercial"
      set url-pattern "com"
   next
   edit "ca"
      set forward-server "server-canada"
      set url-pattern "ca"
   next
   edit "www.google.ca"
      set cache-exemption enable
      set url-pattern "www.google.ca"
   next
end
```

Exempting web sites from web caching

You may want to exempt some URLs from web caching for a number of reasons. For example, if your users access websites that are not compatible with FortiGate web caching you can add the URLs of these web sites to the web caching exempt list. You can add URLs and numeric IP addresses to the web cache exempt list.

You can also add URLs to the web cache exempt list by going to **System > Network > Explicit Proxy** and selecting **Create New**. Add a URL pattern to be exempt and select **Exempt from Cache**.

You can also add URLs and addresses to be exempt from the CLI. Enter the following command to add www.example.com to the web cache exempt list.

```
config web-proxy url-match
   set cache-exemption enable
```

```
      set url-pattern www.example.com
   end
```

Exempting specific files from caching

You can exempt files from being cached, so long as you specify its full URL. Enter the following command to add the URL, with the file extension (in this example, `.exe`), to the web cache exempt list:

```
config web-proxy url-match
   edit "exe"
      set url-pattern "iavs9x.u.avast.com/custom/iavs9x/20160613t1237z/avast_free_
          antivirus_setup_online.exe"
      set cache-exemption enable
   next
end
```

You cannot use wildcards to exempt file extensions in general from caching.

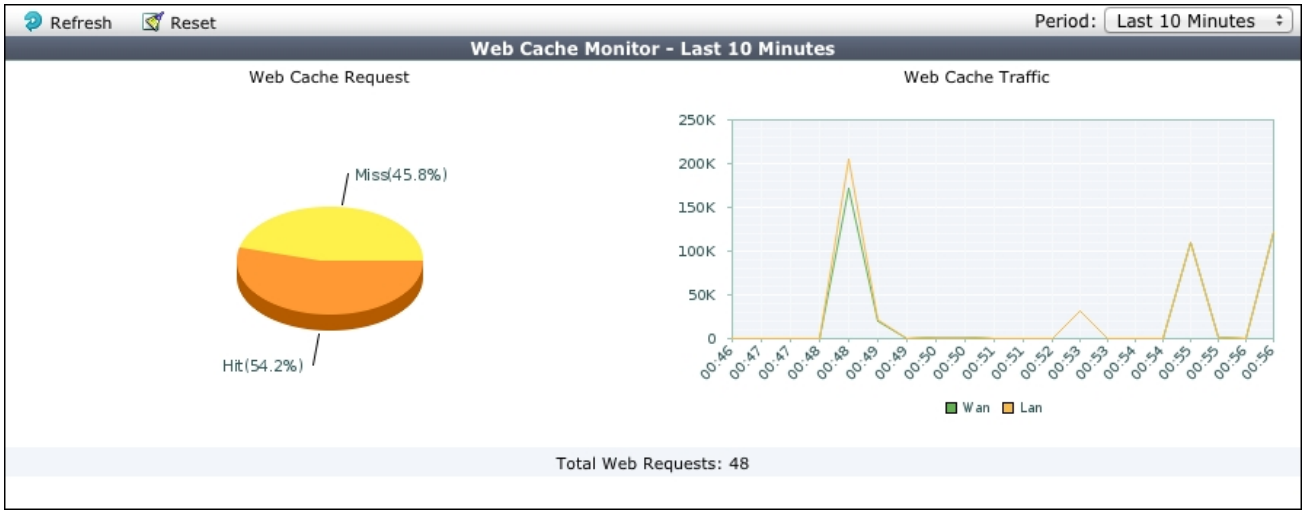
Monitoring Web caching performance

The web cache monitor shows the percentage of web cache requests that retrieved content from the cache (hits) and the percentage that did not receive content from the cache (misses). A higher the number of hits usually indicates that the web cache is being more effective at reducing WAN traffic.

The web cache monitor also shows a graph of web traffic on the WAN and LAN. A lower WAN line on the graph indicates the web cache is reducing traffic on the WAN. The web cache monitor also displays the total number of web requests processed by the web cache.

To view the web cache monitor, go to **WAN Opt. & Cache > Monitor > Cache Monitor**.

Web cache monitor



Example Web caching of HTTP and HTTPS Internet content for users on an internal network

This example describes how to configure web caching of HTTP and HTTPS for users on a private network connecting to the Internet.

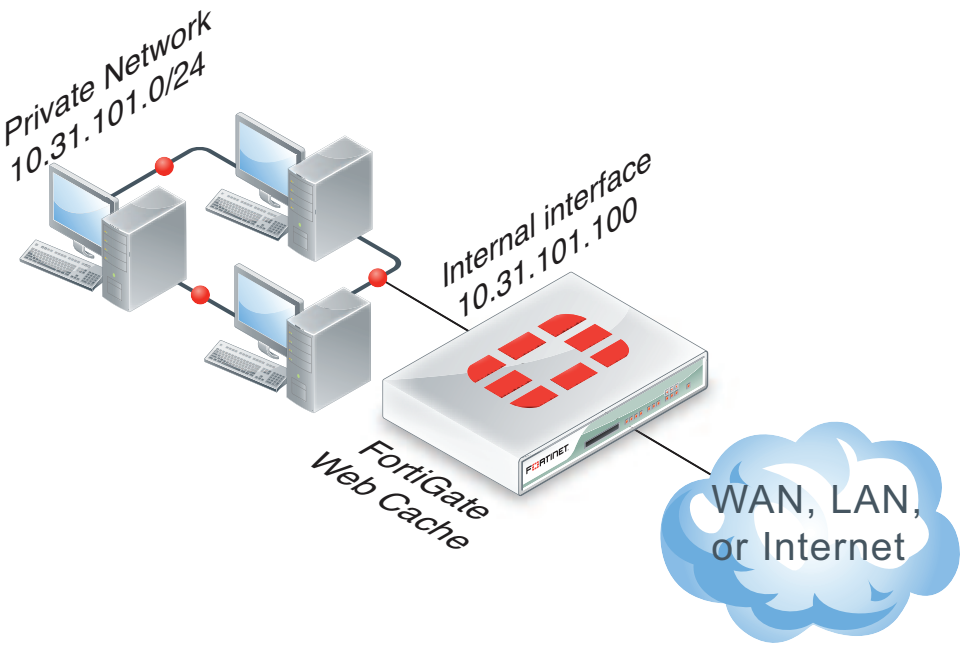
Network topology and assumptions

This example includes a client network with subnet address 10.31.101.0 connecting to web servers on the Internet. All of the users on the private network access the Internet though a single general security policy on the FortiGate unit that accepts all sessions connecting to the Internet. Web caching for HTTP and HTTPS traffic is added to this security policy.

Since users on the private network have unrestricted access to the Internet and can be accessing many web servers the `webcache-https` is set to `any` and users may see error messages on their web browsers when accessing HTTPS content.

Initially, security profiles are not selected so the example caches all HTTP traffic on TCP port 80 and HTTPS traffic on port 443. The example also describes how to configure the security policy to cache HTTP traffic on port 80 and 8080 by adding a proxy options profile that looks for HTTP traffic on TCP ports 80 and 8080. The example also describes how to configure the security policy to cache HTTPS traffic on port 443 and 8443 using the same proxy options profile.

Example web caching topology



General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Add HTTP web caching to the security policy that all users on the private network use to connect to the Internet.
2. Add HTTPS web caching.
3. Add a protocol options profile to look for HTTP traffic on ports 80 and 8080 and HTTPS traffic on ports 443 and 8443 and add this protocol options profile to the security policy.

If you perform any additional actions between procedures, your configuration may have different results.

Configuration Steps - web-based manager

Use the following steps to configure the example configuration from the FortiGate web-based manager.

To add HTTP web caching to a security policy

1. Go to **Policy & Objects > Policy > IPv4** and add a security policy that allows all users on the internal network to access the Internet.

Incoming Interface	Internal
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

2. Select **Enable NAT** and select **Use Destination Interface Address**.
3. Turn on **Web cache**.
4. Select **OK**.

To add HTTPS web caching

1. From the CLI enter the following command to add HTTPS web caching to the policy.

   Assume the index number of the policy is 5.

```
config firewall policy
  edit 5
    set webcache-https any
  end
```

To cache HTTP traffic on port 80 and 8080

1. Go to **Policy & Objects > Policy > Proxy Options** and edit the **default** proxy options profile.

   You could also add a new profile.
2. Under **Protocol Port Mapping** enable **HTTP** and under **Inspection Ports** enter **80,8080**.
3. Go to Policy & Objects > Policy > IPv4, edit the security policy and

To cache HTTPS traffic on ports 443 and 8443

1. Go to **Policy & Objects > Policy > SSL/SSH Inspection** and edit the **certificate-inspection** SSL/SSH inspection profile.

   You could also use the **deep-inspection** profile or add a new profile.
2. Under **SSL Inspection Options** select **Multiple Clients Connecting to Multiple Servers**.
3. Make sure **Inspect All Ports** is not selected.
4. Make sure **HTTPS** is turned on and enter **443,8443**.
5. From the CLI, enter the following command to add the **default** proxy options profile and the **certificate-inspection** SSL SSH profile to the firewall policy.

```
config firewall policy
   edit 5
      set utm-status enable
      set profile-protocol-options default
      set ssl-ssh-profile certificate-inspection
   end
```

You need to use the CLI to add the protocol options profile unless you also add a security profile that uses proxy-based inspection.

Configuration Steps - CLI

Use the following steps to configure the example configuration from the FortiGate CLI.

To add HTTP and HTTPS web caching to a security policy

1. Enter the following command to add a security policy that allows all users on the internal network to access the Internet and that includes web caching of HTTP and HTTPS traffic.

```
config firewall policy
   edit 0
      set srcintf internal
      set srcaddr all
      set dstintf wan1
      set distinf all
      set schedule always
      set service ANY
      set action accept
      set nat enable
      set webcache enable
      set webcache-https any
   end
```

To cache HTTP traffic on port 80 and 8080 and HTTPS traffic on ports 443 and 8443

1. Enter the following command to edit the **default** proxy options profile to configure it to look for HTTP traffic on ports 80 and 8080:

```
config firewall profile-protocol-options
   edit default
      config http
```

```
      set status enable
      set ports 80 8080
   end
```

2. Enter the following command to edit the **certification-inspection** SSL SSH options profile to configure it to look for HTTPS traffic on ports 443 and 8443:

```
config firewall ssl-ssh-profile
   edit certificate-inspection
      config https
         set status certificate-inspection
         set ports 443 8443
      end
```

3. Enter the following command to add the **default** proxy options profile and the **certificate-inspection** SSL SSH profile to the firewall policy.

```
config firewall policy
   edit 5
      set utm-status enable
      set profile-protocol-options default
      set ssl-ssh-profile certificate-inspection
   end
```

Example reverse proxy web caching and SSL offloading for an Internet web server using a static one-to-one virtual IP

This section describes configuring SSL offloading for a reverse proxy web caching configuration using a static one-to-one firewall virtual IP (VIP). While the static one-to-one configuration described in this example is valid, its also common to change the destination port of the unencrypted HTTPS traffic to a commonly used HTTP port such as 8080 using a port forwarding virtual IP.

Network topology and assumptions

In this configuration, clients on the Internet use HTTP and HTTPS to browse to a web server that is behind a FortiGate unit. A policy added to the FortiGate unit forwards the HTTP traffic to the web server. The policy also offloads HTTPS decryption and encryption from the web server so the web server only sees HTTP traffic.

The FortiGate unit also caches HTTP and HTTPS pages from the web server so when users access cached pages the web server does not see the traffic. Replies to HTTPS sessions are encrypted by the FortiGate unit before returning to the clients.

In this configuration, the FortiGate unit is operating as a web cache in reverse proxy mode. Reverse proxy caches can be placed directly in front of a web server. Web caching on the FortiGate unit reduces the number of requests that the web server must handle, therefore leaving it free to process new requests that it has not serviced before.

Using a reverse proxy configuration:

- avoids the capital expense of additional web servers by increasing the capacity of existing servers
- serves more requests for static content from web servers
- serves more requests for dynamic content from web servers
- reduces operating expenses including the cost of bandwidth required to serve content
- accelerates the response time of web servers and of page download times to end users.

When planning a reverse proxy implementation, the web server's content should be written so that it is “cache aware” to take full advantage of the reverse proxy cache.

In reverse proxy mode, the FortiGate unit functions more like a web server for clients on the Internet. Replicated content is delivered from the proxy cache to the external client without exposing the web server or the private network residing safely behind the firewall.

In this example, the site URL translates to IP address 192.168.10.1, which is the port2 IP address of the FortiGate unit. The port2 interface is connected to the Internet.

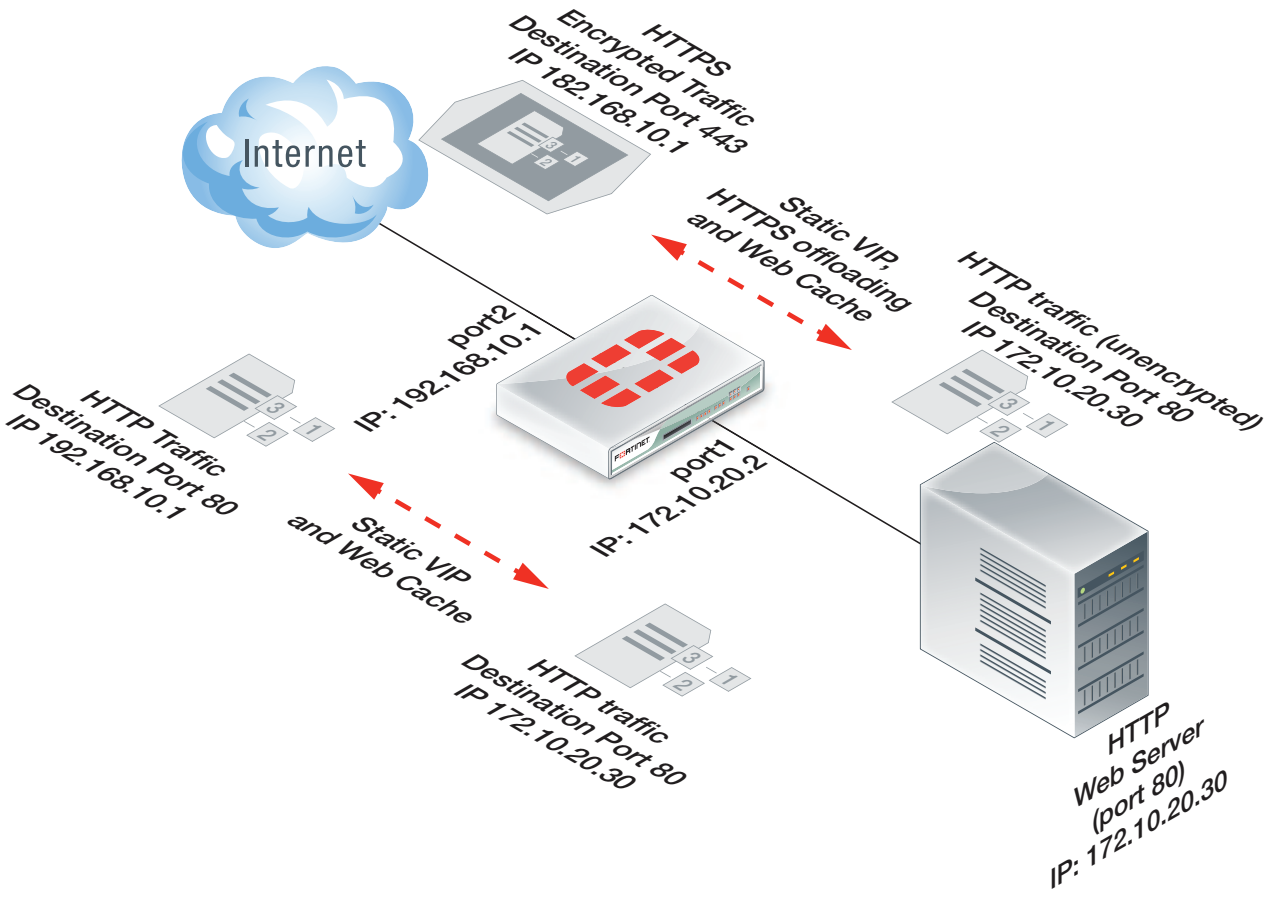
This example assumes that all HTTP traffic uses port 80 and all HTTPS traffic uses port 443.

The FortiGate unit includes the web server CA and an SSL server configuration for IP address 172.10.20.30 and port to 443. The name of the file containing the CA is Rev_Proxy_Cert_1.crt.

The destination address of incoming HTTP and HTTPS sessions is translated to the IP address of the web server using a static one-to-one virtual IP that performs destination address translation (DNAT) for the HTTP packets. The DNAT translates the destination address of the packets from 192.168.10.1 to 172.10.20.30 but does not change the destination port number.

When the SSL server on the FortiGate unit decrypts the HTTPS packets their destination port is changed to port 80.

Reverse proxy web caching and SSL offloading for an Internet web server using static one-to-one virtual IPs



General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the FortiGate unit as a reverse proxy web cache server.
2. Configure the FortiGate unit for SSL offloading of HTTPS traffic.
3. Add an SSL server to offload SSL encryption and decryption for the web server.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuration steps - web-based manager

To configure the FortiGate unit as a reverse proxy web cache server

1. Go to **Policy & Objects > Objects > Virtual IPs** and select **Create New** to add a static NAT virtual IP that translates destination IP addresses from 192.168.10.1 to 172.10.20.30 (and does not translate destination ports):

VIP Type	IPv4 VIP
Name	Reverse_proxy_VIP
Interface	port2
Type	Static NAT
Source Address Filter	Do not select.
External IP Address/Range	192.168.10.1
Mapped IP Address/Range	172.10.20.30
Port Forwarding	Do not select.

2. Select **OK**.
3. Go to **Policy & Objects > Objects > IPv4** and select **Create New** to add a port2 to port1 security policy that accepts HTTP and HTTPS traffic from the Internet.

   Do not select security profiles. Set the destination address to the virtual IP. You do not have to enable NAT.

Incoming Interface	port2
Source Address	all
Outgoing Interface	port1
Destination Address	Reverse_proxy_VIP
Schedule	always

Service	HTTP HTTPS
Action	ACCEPT

4. Turn on **Web Cache**.
5. Select **OK**.
6. From the CLI enter the following command to add HTTPS web caching to the security policy

   Assume the index number of the policy is 5.

```
config firewall policy
   edit 5
      set webcache-https ssl-server
   end
```

To configure the FortiGate unit to offload SSL encryption and cache HTTPS content

1. Go to **System > Certificates > Local Certificates** and select **Import** to import the web server's CA.

   For **Type**, select **Local Certificate**. Select the **Browse** button to locate the file (example file name: Rev_Proxy_Cert_1.crt).

   The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.
2. Select **OK** to import the certificate.
3. From the CLI, enter the following command to add the SSL server and to add the server's certificate to the SSL server.

   The SSL server `ip` must match the destination address of the SSL traffic after being translated by the virtual IP (172.10.20.30) and the SSL server `port` must match the destination port of the SSL traffic (443). The SSL server operates in half mode since it performs a single-step conversion (HTTPS to HTTP or HTTP to HTTPS).

```
config firewall ssl-server
   edit rev_proxy_server
      set ip 172.10.20.30
      set port 443
      set ssl-mode half
      set ssl-cert Rev_Proxy_Cert_1
   end
```

Configuration steps - CLI

To configure the FortiGate unit as a reverse proxy web cache server

1. Enter the following command to add a static NAT virtual IP that translates destination IP addresses from 192.168.10.1 to 172.10.20.30 (and does not translate destination ports):

```
config firewall vip
   edit Reverse_proxy_VIP
      set extintf port2
      set type static-nat
      set extip 192.168.10.1
      set mappedip 172.10.20.30
   end
```

2. Enter the following command to add a port2 to port1 security policy that accepts HTTP and HTTPS traffic from the Internet. Enable web caching and HTTPS web caching.

   Do not select security profiles. Set the destination address to the virtual IP. You do not have to enable NAT.

```
config firewall policy
   edit 0
      set srcintf port2
      set srcaddr all
      set dstintf port1
      set dstaddr Reverse_proxy_VIP
      set schedule always
      set service HTTP HTTPS
      set action accept
      set webcache enable
      set webcache-https ssl-server
   end
```

To add an SSL server to offload SSL encryption and decryption for the web server

1. Place a copy of the web server's CA (file name Rev_Proxy_Cert_1.crt) in the root folder of a TFTP server.
2. Enter the following command to import the web server's CA from a TFTP server. The IP address of the TFTP server is 10.31.101.30:

```
execute vpn certificate local import tftp Rev_Proxy_Cert_1.crt 10.31.101.30
```

   The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

3. From the CLI, enter the following command to add the SSL server.

   The SSL server `ip` must match the destination address of the SSL traffic after being translated by the virtual IP (172.10.20.30) and the SSL server `port` must match the destination port of the SSL traffic (443). The SSL server operates in half mode since it performs a single-step conversion (HTTPS to HTTP or HTTP to HTTPS).

```
config firewall ssl-server
   edit rev_proxy_server
      set ip 172.10.20.30
      set port 443
      set ssl-mode half
      set ssl-cert Rev_Proxy_Cert_1
   end
```

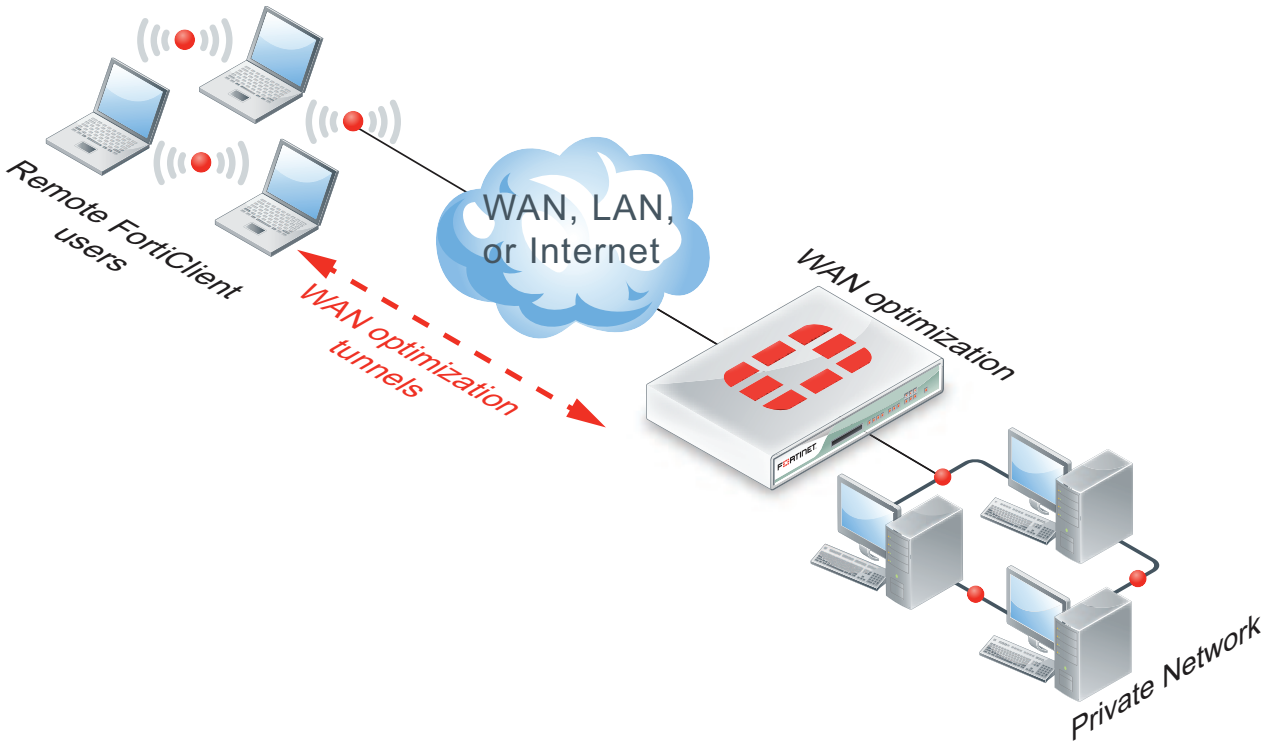
4. Configure other `ssl-server` settings that you may require for your configuration.

FortiClient WAN optimization

FortiClient WAN optimization supports protocol optimization and byte caching in IPsec VPN and SSL VPN tunnels between FortiClient and a FortiGate unit. To add WAN optimization to FortiClient, configure FortiClient Advanced settings and enable WAN optimization. This setting can then apply WAN optimization to any IPsec or SSL VPN tunnel between FortiClient and FortiGate, if the FortiGate IPsec or SSL VPN configuration also includes WAN optimization.

When FortiClient with WAN optimization enabled attempts to connect a server-side FortiGate unit, FortiClient automatically detects if WAN optimization has been added to the FortiGate tunnel configuration. If WAN optimization is detected and FortiClient can successfully negotiate with the FortiGate unit, WAN optimization starts.

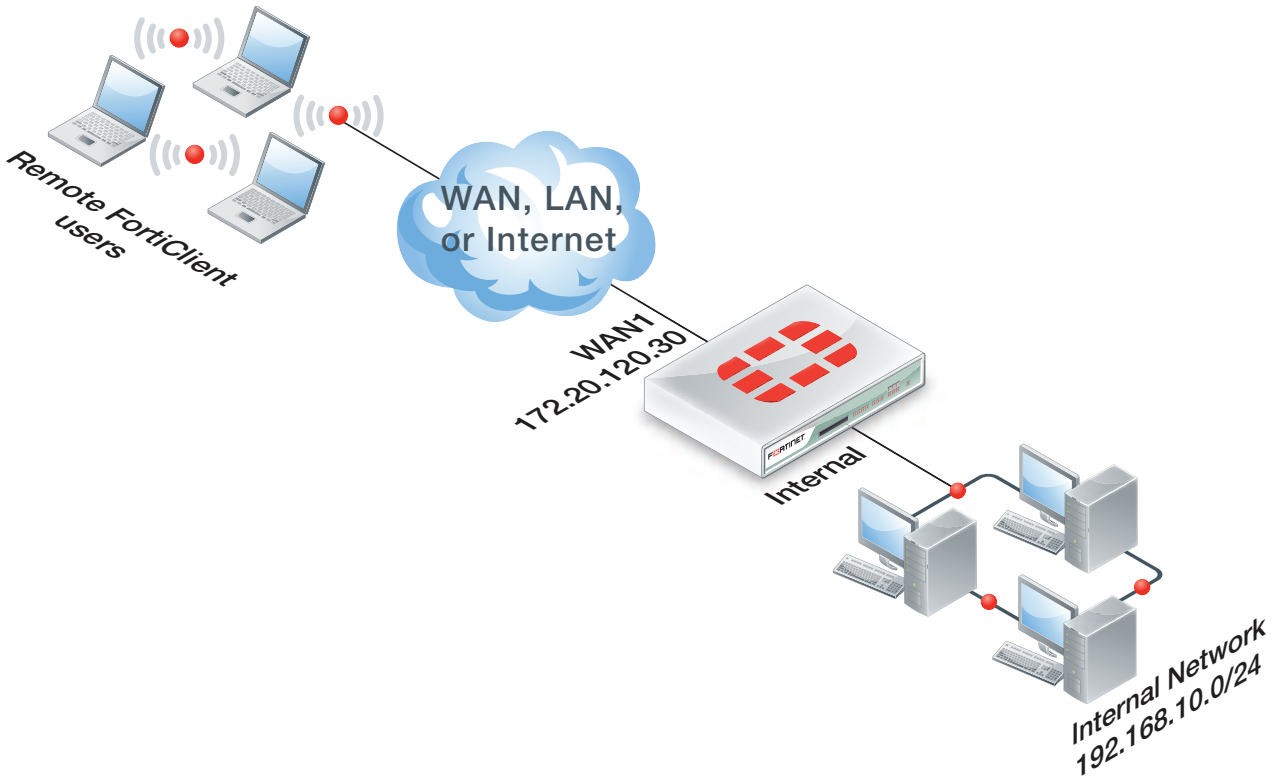
FortiClient WAN optimization topology



FortiClient WAN optimization over IPsec VPN configuration example

This example shows how to add WAN optimization to a FortiClient IPsec VPN. The IPsec VPN tunnel allows remote FortiClient users to connect to the internal network behind the FortiGate unit.

Example FortiClient WAN optimization configuration



To configure the FortiGate unit

Because computers running FortiClient can have IP addresses that change often, it is usually not practical to add FortiClient peers to the FortiGate WAN optimization peer list. Instead, a FortiGate unit that accepts WAN optimization tunnel requests from FortiClient is usually configured to accept any peer. This example does this by adding a WAN optimization authentication group with **Peer acceptance** set to **Accept Any Peer**.

In addition this example includes a **wanopt** to **internal** policy to allow WAN optimization traffic reach the internal network. Finally passive WAN optimization is added to the ssl.root policy because WAN optimization is accepting traffic from the IPsec VPN tunnel.

1. Go to **WAN Opt. & Cache > WAN Opt. Peers > Authentication Groups** and select **Create New**.
2. Configure the WAN optimization authentication group:

Name	auth-fc
Authentication Method	Certificate
Certificate	Fortinet_Firmware
Peer Acceptance	Accept Any Peer

3. Select **OK**.

4. Go to **WAN Opt. & Cache > WAN Opt. Profiles > Profiles** and select **Create New** (select the + button).
5. Add a profile for FortiClient WAN optimization sessions:

Name	Fclient_Pro
Transparent Mode	Select
Authentication Group	auth-fc

6. Select any Protocols and any settings for each protocol.
7. Select **OK**.
8. Go to **Policy& Objects > Objects > Addresses** and select **Create New** to add a firewall address for the internal network that FortiClient users can access.

Category	Address
Address Name	Internal-Server-Net
Type	IP Range
Subnet / IP Range	192.168.10.0/24
Interface	internal

9. Enter the following CLI command to add an explicit proxy policy to accept WAN optimization tunnel connections.

```
configure firewall explicit-proxy-policy
   edit 0
      set proxy wanopt
      set dstintf internal
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
   next
end
```

To set up IPsec VPN to support WAN optimization

1. Go to **VPN > IPsec > Wizard**, enter a **Name** for the IPsec VPN and select **Dialup - FortiClient (Windows, Mac OS, Android)**.
2. Follow the wizard steps to configure the VPN. No special WAN optimization settings are required.
3. Go to **Policy & Objects > Policy > IPv4** and edit the policy created by the wizard.

   This policy has the IPsec VPN interface created by the wizard as the source interface.
4. Turn on **WAN Optimization** and configure the following settings:

Enable WAN Optimization	passive
Passive Option	default

5. Select **OK**.

To configure FortiClient and start the WAN optimization SSL VPN connection

1. Open FortiClient, configure **Advanced** settings, and select **Enable WAN optimization**.
2. Add a new IPsec VPN connection.

   Set the Server to the WAN1 IP address of the FortiGate unit (172.20.120.30 in this example).

   No other settings are required for this example. You can add authentication in the form of a user name and password if required by the FortiGate unit.
3. Start the IPsec VPN tunnel.

   You should be connected to the IPsec VPN tunnel and traffic in it should be optimized.

The FortiGate explicit web proxy

You can use the FortiGate explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP, and HTTPS traffic one or more FortiGate interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI you can also configure the explicit web proxy to support SOCKS sessions from a web browser.

The explicit web and FTP proxies can be operating at the same time on the same or on different FortiGate interfaces.

If explicit web proxy options are not visible on the web-based manager, go to **System > Config > Features** and turn on **Explicit Proxy**.

In most cases you would configure the explicit web proxy for users on a network by enabling the explicit web proxy on the FortiGate interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiGate interface connected to their network. Users could also enter the PAC URL into their web browser PAC configuration to automate their web proxy configuration using a PAC file stored on the FortiGate unit.

Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

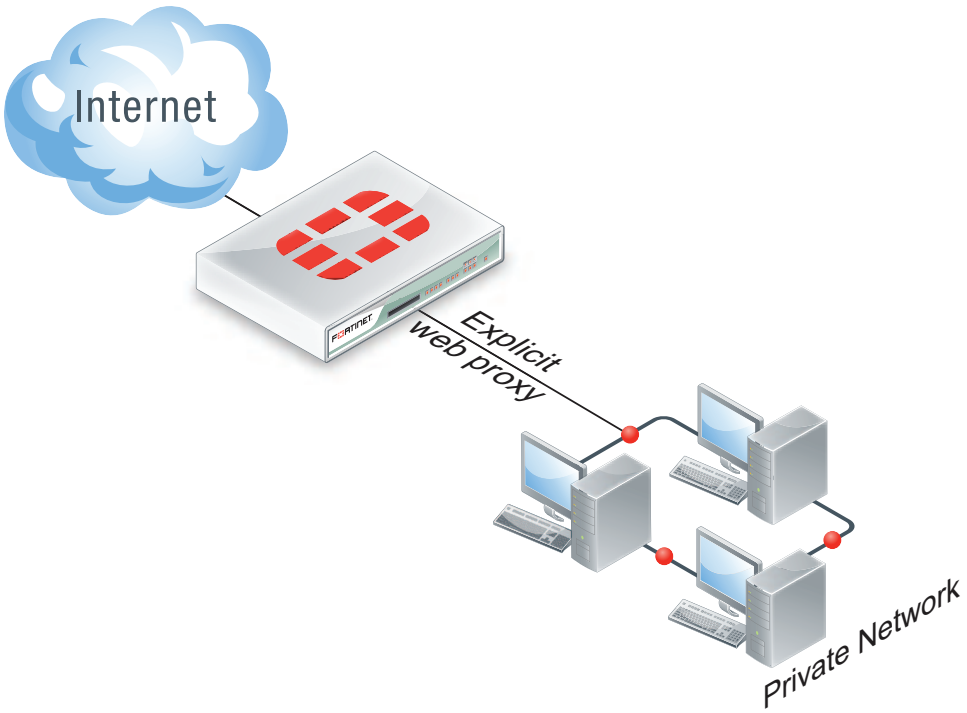
If the FortiGate unit is operating in Transparent mode, users would configure their browsers to use a proxy server with the FortiGate management IP address.

If the FortiGate unit is operating with multiple VDOMs the explicit web proxy is configured for each VDOM.

The web proxy receives web browser sessions to be proxied at FortiGate interfaces with the explicit web proxy enabled. The web proxy uses FortiGate routing to route sessions through the FortiGate unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the FortiGate unit is operating in Transparent mode the explicit web proxy changes the source addresses to the management IP address. You can configure the explicit web proxy to keep the original client IP address. See Preventing the explicit web proxy from changing source addresses on page 2914.

For more information about explicit web proxy sessions, see Explicit web proxy sessions and user limits on page 2920.

Example explicit web proxy topology



To allow all explicit web proxy traffic to pass through the FortiGate unit you can set the explicit web proxy default firewall policy action to accept. However, in most cases you would want to use security policies to control explicit web proxy traffic and apply security features such as access control/authentication, virus scanning, web filtering, application control, and traffic logging. You can do this by keeping the default explicit web proxy security policy action to deny and then adding web-proxy security policies.

You can also change the explicit web proxy default security policy action to accept and add explicit web proxy security policies. If you do this, sessions that match web-proxy security policies are processed according to the security policy settings. Connections to the explicit web proxy that do not match a web-proxy security policy are allowed with no restrictions or additional security processing. This configuration is not recommended and is not a best practice.

Web-proxy policies can selectively allow or deny traffic, apply authentication, enable traffic logging, and use security profiles to apply virus scanning, web filtering, IPS, application control, DLP, and SSL/SSH inspection to explicit web proxy traffic.

You cannot configure IPsec, SSL VPN, or Traffic shaping for explicit web proxy traffic. Web Proxy policies can only include firewall addresses not assigned to a FortiGate unit interface or with interface set to **Any**. (On the web-based manager you must set the interface to **Any**. In the CLI you must `unset` the `associated-interface`.)

Authentication of explicit web proxy sessions uses HTTP authentication and can be based on the user's source IP address or on cookies from the user's web browser. For more information, see Explicit web proxy authentication on page 2909.

To use the explicit web proxy, users must add the IP address of a FortiGate interface on which the explicit web proxy is enabled and the explicit web proxy port number (default 8080) to the proxy configuration settings of their web browsers.

On FortiGate units that support it, you can also enable web caching for explicit web proxy sessions.

General explicit web proxy configuration steps

You can use the following general steps to configure the explicit web proxy.

To enable the explicit web proxy - web-based manager:

1. Go to **System > Network > Explicit Proxy**. Select **HTTP/HTTPS** beside **Enable Explicit Web Proxy** to turn on the explicit web proxy for IPv4 HTTP and HTTPS traffic.

   You can also select FTP to enable the web proxy for FTP over HTTP sessions in a web browser (not an FTP client) and PAC to enable automatic proxy configuration.

   You can also optionally change the HTTP port that the proxy listens on (the default is 8080) and optionally specify different ports for HTTPS, FTP, and PAC.
2. Optionally select **Enable IPv6 Explicit Proxy** to turn on the explicit web proxy for IPv6 traffic.

If you enable both the IPv4 and the IPv6 explicit web proxy you can combine IPv4 and IPv6 addresses in a single explicit web proxy policy to allow both IPv4 and IPv6 traffic through the proxy.

3. Select **Apply**.

   The default explicit web proxy configuration has **Default Firewall Policy Action** set to Deny and requires you to add a security policy to allow access to the explicit web proxy. This configuration is recommended as a best practice because you can use security policies to control access to the explicit web proxy and also apply security features such as logging, UTM, and authentication (by adding identity-based policies).
4. Go to **System > Network > Interface** and select one or more interfaces for which to enable the explicit web proxy. Edit the interface and select **Enable Explicit Web Proxy**.

Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address. If you enable the proxy on such an interface make sure authentication is required to use the proxy.

5. Go to **Policy & Objects > Objects > Addresses** and select **Create New** to add a firewall address that matches the source address of packets to be accepted by the explicit proxy.

Category	Address
Name	Internal_subnet
Type	IP Range

Subnet / IP Range	10.31.101.1 - 10.31.101.255
Interface	any*

*The **Interface** must be set to **Any**.

You can also set the **Type** to **URL Pattern (Explicit Proxy)** to add a destination URL that is only used by the explicit proxy. For example, to create an explicit policy that only allows access to Fortinet.com:

Category	Address
Name	Fortinet-web-sites
Type	URL Pattern (Explicit Proxy)
URL Pattern	fortinet.com
Interface	any

6. Go to **Policy & Objects > Policy > Explicit Proxy** and select **Create New.** Configure the policy as required to accept the traffic that you want to be allowed to use the explicit web proxy.

   The source address of the policy must match the client's source IP addresses. The interface of this firewall address must be set to **any**.

   The destination address of the policy should match the IP addresses of web sites that clients are connecting to. Usually the destination address would be **all** if proxying Internet web browsing. You could also specify a URL firewall address to limit the policy to allowing access to this URL.

   If **Default Firewall Policy Action** is set to **Deny**, traffic sent to the explicit web proxy that is not accepted by a web-proxy policy is dropped. If **Default Firewall Policy Action** is set to **Allow** then all web-proxy sessions that don't match with a security policy are allowed.

   For example, the following security policy allows users on an internal network to access fortinet.com websites through the wan1 interface of a FortiGate unit.

Explicit Proxy Type	Web
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	Fortinet-web-sites
Schedule	always
Action	ACCEPT

   Add security profiles as required.

7. Select Create New to add another explicit web proxy and set the **Action** to **AUTHENTICATE** to require authentication to access the explicit web proxy. For example:

Explicit Proxy Type	Web
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	Fortinet-web-sites
Schedule	always
Action	AUTHENTICATE

Select **Create New** to add an **Authentication Rule** and configure the rule as follows:

Groups	Proxy-Group
Source User(s)	(optional)
Schedule	always

Add security profiles as required and select **OK**.

You can add multiple user identity policies to apply different authentication for different user groups and users and also apply different UTM and logging settings for different user groups.

You can change the **User Authentication Options** if required. In most cases you can accept the defaults.

8. Optionally enable Web Caching.
9. Select **OK**.

To enable the explicit web proxy - CLI:

1. Enter the following command to turn on the IPv4 and IPv6 explicit web proxy for HTTP and HTTPS traffic.

```
config web-proxy explicit
   set status enable
   set ipv6-status enable
end
```

You can also enter the following command to enable the web proxy for FTP sessions in a web browser.

```
config web-proxy explicit
   set ftp-over-http enable
end
```

The default explicit web proxy configuration has `sec-default-action` set to `deny` and requires you to add a security policy to allow access to the explicit web proxy.

2. Enter the following command to enable the explicit web proxy for the internal interface.

```
config system interface
   edit internal
      set explicit-web-proxy enable
   end
end
```

3. Use the following command to add a firewall address that matches the source address of users who connect to the explicit web proxy.

```
config firewall address
   edit Internal_subnet
      set type iprange
      set start-ip 10.31.101.1
      set end-ip 10.31.101.255
   end
```

The source address for a web-proxy security policy cannot be assigned to a FortiGate interface.

4. Optionally use the following command to add a destination URL that is only used by the explicit proxy. For example, to create an explicit policy that only allows access to Fortinet.com:

```
config firewall address
   edit Fortinet-web-sites
      set type url
      set url fortinet.com
   end
```

5. Use the following command to add an explicit web proxy policy that allows all users on the internal subnet to use the explicit web proxy for connections through the wan1 interface to the Internet.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set dstintf wan1
      set scraddr Internal_subnet
      set dstaddr all
      set action accept
      set service webproxy
      set schedule always
end
```

6. Use the following command to add an explicit web proxy policy that allows authenticated users on the internal subnet to use the explicit web proxy for connections through the wan1 interface to the Internet.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set dstintf wan1
      set scraddr Internal_subnet
      set dstaddr Fortinet-web-sites
      set action accept
      set service webproxy
      set schedule always
      set identity-based enable
         config identity-based-policy
            edit 1
               set groups Proxy-group
               set schedule always
      end
end
```

7. Use the following command to change global web proxy settings, for example to set the maximum request length for the explicit web proxy to 10:

```
config web-proxy global
   set max-request-length 10
end
```

Proxy auto-config (PAC) configuration

A proxy auto-config (PAC) file defines how web browsers can choose a proxy server for receiving HTTP content. PAC files include the FindProxyForURL(url, host) JavaScript function that returns a string with one or more access method specifications. These specifications cause the web browser to use a particular proxy server or to connect directly.

To configure PAC for explicit web proxy users, you can use the port that PAC traffic from client web browsers use to connect to the explicit web proxy. explicit web proxy users must configure their web browser's PAC proxy settings to use the PAC port.

PAC File Content

You can edit the default PAC file from the web-based manager or use the following command to upload a custom PAC file:

```
config web-proxy explicit
   set pac-file-server-status enable
   set pac-file-data <pac_file_str>
end
```

Where <pac_file_str> is the contents of the PAC file. Enter the PAC file text in quotes. You can copy the contents of a PAC text file and paste the contents into the CLI using this option. Enter the command followed by two sets of quotes then place the cursor between the quotes and paste the file content.

The maximum PAC file size is 256 kbytes. If your FortiGate unit is operating with multiple VDOMs each VDOM has its own PAC file. The total amount of FortiGate memory available to store all of these PAC files 2 MBytes. If this limit is reached you will not be able to load any additional PAC files.

You can use any PAC file syntax that is supported by your users's browsers. The FortiGate unit does not parse the PAC file.

To use PAC, users must add an automatic proxy configuration URL (or PAC URL) to their web browser proxy configuration. The default FortiGate PAC file URL is:

```
http://<interface_ip>:<PAC_port_int>/<pac_file_str>
```

For example, if the interface with the explicit web proxy has IP address 172.20.120.122, the PAC port is the same as the default HTTP explicit web proxy port (8080) and the PAC file name is proxy.pac the PAC file URL would be:

```
http://172.20.120.122:8080/proxy.pac
```

From the CLI you can use the following command to display the PAC file URLs:

```
get web-proxy explicit
```

Unknown HTTP version

You can select the action to take when the proxy server must handle an unknown HTTP version request or message. Set unknown HTTP version to Reject or Best Effort. Best Effort attempts to handle the HTTP traffic as best as it can. Reject treats known HTTP traffic as malformed and drops it. The Reject option is more secure.

Authentication realm

You can enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces enclose it in quotes. When a user authenticates with the explicit web

proxy the HTTP authentication dialog includes the realm so you can use the realm to identify the explicitly web proxy for your users.

Other explicit web proxy options

You can change the following explicit web proxy options as required by your configuration.

HTTP port, HTTPS port, FTP port, PAC port	The TCP port that web browsers use to connect to the explicit proxy for HTTP, HTTPS, FTP and PAC services. The default port is 8080 for all services. By default HTTPS, FTP. and PAC use the same port as HTTP. You can change any of these ports as required. Users configuring their web browsers to use the explicit web proxy should add the same port numbers to their browser configurations.
Proxy FQDN	Enter the fully qualified domain name (FQDN) for the proxy server. This is the domain name to enter into browsers to access the proxy server.
Max HTTP request length	Enter the maximum length of an HTTP request in Kbytes. Larger requests will be rejected.
Max HTTP message length	Enter the maximum length of an HTTP message in Kbytes. Larger messages will be rejected.

Configuring an external IP address for the IPv4 explicit web proxy

You can use the following command to set an external IP address (or pool) that will be used by the explicit web proxy policy.

```
config web-proxy explicit
   set status enable
   set outgoing-ip <ip1> <ip2> ... <ipN>
end
```

Configuring an external IP address for the IPv6 explicit web proxy

You can use the following command to set an external IP address (or pool) that will be used by the explicit web proxy policy.

```
config web-proxy explicit
   set status enable
   set outgoing-ipv6 <ip1> <ip2> ... <ipN>
end
```

Restricting the IP address of the IPv4 explicit web proxy

You can use the following command to restrict access to the explicit web proxy using only one IP address. The IP address that you specify must be the IP address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit FTP proxy is enabled on an interface with multiple IP addresses.

For example, to require uses to connect to the IP address 10.31.101.100 to connect to the explicit HTTP proxy:

```
config web-proxy explicit
   set incoming-ip 10.31.101.100
end
```

Restricting the outgoing source IP address of the IPv4 explicit web proxy

You can use the following command to restrict the source address of outgoing web proxy packets to a single IP address. The IP address that you specify must be the IP address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit HTTP proxy is enabled on an interface with multiple IP addresses.

For example, to restrict the outgoing packet source address to 172.20.120.100:

```
config http-proxy explicit
   set outgoing-ip 172.20.120.100
end
```

Restricting the IP address of the explicit IPv6 web proxy

You can use the following command to restrict access to the IPv6 explicit web proxy to use only one IP6 IP address. The IPv6 address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit web proxy is enabled on an interface with multiple IPv6 addresses.

For example, to require uses to connect to the IPv6 address 2001:db8:0:2::30 to connect to the explicit IPv6 HTTP proxy:

```
config web-proxy explicit
   set incoming-ipv6 2001:db8:0:2::30
end
```

Restricting the outgoing source IP address of the IPv6 explicit web proxy

You can use the following command to restrict the source address of outgoing web proxy packets to a single IPv6 address. The IP address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit HTTP proxy is enabled on an interface with multiple IPv6 addresses.

For example, to restrict the outgoing packet source address to 2001:db8:0:2::50:

```
config http-proxy explicit
   set outgoing-ip6 2001:db8:0:2::50
end
```

Proxy chaining (web proxy forwarding servers)

For the explicit web proxy you can configure web proxy forwarding servers to use proxy chaining to redirect web proxy sessions to other proxy servers. Proxy chaining can be used to forward web proxy sessions from the FortiGate unit to one or more other proxy servers on your network or on a remote network. You can use proxy chaining to integrate the FortiGate explicit web proxy with an web proxy solution that you already have in place.

A FortiGate unit can forward sessions to most web proxy servers including a remote FortiGate unit with the explicit web proxy enabled. No special configuration of the explicit web proxy on the remote FortiGate unit is required.

You can deploy the explicit web proxy with proxy chaining in an enterprise environment consisting of small satellite offices and a main office. If each office has a FortiGate unit, users at each of the satellite offices can use

their local FortiGate unit as an explicit web proxy server. The satellite office FortiGate units can forward explicit web proxy sessions to an explicit web proxy server at the central office. From here the sessions can connect to web servers on the Internet.

FortiGate proxy chaining does not support authenticating with the remote forwarding server.

Adding a web proxy forwarding server

To add a forwarding server, select **Create New** in the **Web Proxy Forwarding Servers** section of the **Explicit Proxy** page by going to **System > Network > Explicit Proxy**.

Server Name	Enter the name of the forwarding server.
Proxy Address	Enter the IP address of the forwarding server.
Proxy Address Type	Select the type of IP address of the forwarding server. A forwarding server can have an FQDN or IP address.
Port	Enter the port number on which the proxy receives connections. Traffic leaving the FortiGate explicit web proxy for this server has its destination port number changed to this number.
Server Down action	Select what action the explicit web proxy to take if the forwarding server is down. **Block** means if the remote server is down block traffic. **Use Original Server** means do not forward traffic to the forwarding sever but instead forward it from the FortiGate to its destination. In other words operate as if there is no forwarding server configured.
Enable Health Monitor	Select to enable health check monitoring and enter the address of a remote site. See "Web proxy forwarding server monitoring and health checking".
Health Check Monitor Site	

Use the following CLI command to add a web proxy forwarding server named `fwd-srv` at address `proxy.example.com` and port 8080.

```
config web-proxy forward-server
   edit fwd-srv
      set addr-type fqdn
      set fqdn proxy.example.com

      set port 8080
   end
```

Web proxy forwarding server monitoring and health checking

By default, a FortiGate unit monitors web proxy forwarding server by forwarding a connection to the remote server every 10 seconds. If the remote server does not respond it is assumed to be down. Checking continues and when the server does send a response the server is assumed to be back up. If you configure health checking, every 10

seconds the FortiGate unit attempts to get a response from a web server by connecting through the remote forwarding server.

You can configure health checking for each remote server and specify a different website to check for each one.

If the remote server is found to be down you can configure the FortiGate unit to block sessions until the server comes back up or to allow sessions to connect to their destination, bypassing the remote forwarding server. You cannot configure the FortiGate unit to fail over to another remote forwarding server.

Configure the server down action and enable health monitoring from the web-based manager by going to **System > Network > Explicit Proxy**, selecting a forwarding server, and changing the server down action and changing the health monitor settings.

Use the following CLI command to enable health checking for a web proxy forwarding server and set the server down option to bypass the forwarding server if it is down.

```
config web-proxy forward-server
   edit fwd-srv
      set healthcheck enable
      set monitor http://example.com
      set server-down-option pass
   end
```

Grouping forwarding servers and load balancing traffic to them

You can add multiple web proxy forwarding servers to a forwarding server group and then add the server group to an explicit web proxy policy instead of adding a single server. Forwarding server groups are created from the FortiGate CLI but can be added to policies from the web-based manager (or from the CLI).

When you create a forwarding server group you can select a load balancing method to control how sessions are load balanced to the forwarding servers in the server group. Two load balancing methods are available:

- **Weighted** load balancing sends more sessions to the servers with higher weights. You can configure the weight for each server when you add it to the group.
- **Least-session** load balancing sends new sessions to the forwarding server that is processing the fewest sessions.

When you create a forwarding server group you can also enable **affinity**. Enable affinity to have requests from the same client processed by the same server. This can reduce delays caused by using multiple servers for a single multi-step client operation. Affinity takes precedence over load balancing.

You can also configure the behavior of the group if all of the servers in the group are down. You can select to **block** traffic or you can select to have the traffic **pass** through the FortiGate explicit proxy directly to its destination instead of being sent to one of the forwarding servers.

Use the following command to add a forwarding server group that users weighted load balancing to load balance traffic to three forwarding servers. Server weights are configured to send most traffic to server2. The group has affinity enabled and blocks traffic if all of the forward servers are down:

```
config web-proxy forward-server
   edit server_1
      set ip 172.20.120.12
      set port 8080
   next
   edit server_2
      set ip 172.20.120.13
      set port 8000
   next
   edit server_3
```

```
        set ip 172.20.120.14
        set port 8090
    next
    end
config web-proxy forward-server-group
    edit New-fwd-group
        set affinity enable
        set ldb-method weight
        set group-down-option block
            config server-list
                edit server_1
                    set weight 10
                next
                edit server_2
                    set weight 40
                next
                edit server_3
                    set weight 10
                next
    end
```

Adding proxy chaining to an explicit web proxy policy

You enable proxy chaining for web proxy sessions by adding a web proxy forwarding server or server group to an explicit web proxy policy. In a policy you can select one web proxy forwarding server or server group. All explicit web proxy traffic accepted by this security policy is forwarded to the specified web proxy forwarding server or server group.

To add an explicit web proxy forwarding server - web-based manager:

1. Go to **Policy & Objects > Policy > Explicit Proxy** and select **Create New**.
2. Configure the policy:

Explicit Proxy Type	Web
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Action	ACCEPT
Web Proxy Forwarding Server	Select, fwd-srv

3. Select **OK** to save the security policy.

To add an explicit web proxy forwarding server - CLI:

1. Use the following command to add a security policy that allows all users on the 10.31.101.0 subnet to use the explicit web proxy for connections through the wan1 interface to the Internet. The policy forwards web proxy sessions to a remote forwarding server named `fwd-srv`

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set dstintf wan1
      set scraddr Internal_subnet
      set dstaddr all
      set action accept
      set schedule always
      set webproxy-forward-server fwd-srv
   end
```

Explicit web proxy authentication

You can add authentication to explicit web proxy policies to control access to the explicit web proxy and to identify users and apply different UTM features to different users.

Authentication of web proxy sessions uses HTTP basic and digest authentication as described in RFC 2617 (HTTP Authentication: Basic and Digest Access Authentication) and prompts the user for credentials from the browser allowing individual users to be identified by their web browser instead of IP address. HTTP authentication allows the FortiGate unit to distinguish between multiple users accessing services from a shared IP address.

You can also select IP-based authentication to authenticate users according to their source IP address in the same way as normal firewall policies.

IP-Based authentication

IP-based authentication applies authentication by source IP address. For the explicit web proxy, IP authentication is compatible with basic, digest, NTLM, FSSO, or RSSO authentication methods. Once a user authenticates, all sessions to the explicit web proxy from that user's IP address are assumed to be from that user and are accepted until the authentication timeout ends or the session times out.

This method of authentication is similar to standard (non-web proxy) firewall authentication and may not produce the desired results if multiple users share IP addresses (such as in a network that uses virtualization solutions or includes a NAT device between the users and the explicit web proxy).

To configure IP-based authentication, add an explicit web proxy security policy, set the **Action to AUTHENTICATION**, and select **Enable IP Based Authentication** is selected.

Use the following CLI command to add IP-based authentication to a web proxy security policy. IP-based authentication is selected by setting `ip-based` to `enable`.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set scraddr User_network
      set dstintf port1
      set dstaddr all
      set action accept
      set identity-based enable
      set ip-based enable
         config identity-based-policy
            edit 0
               set groups Internal_users
               set users dwhite rlee
               set schedule always
            end
```

Per session authentication

If you don't select **IP Based** the explicit web proxy applies HTTP authentication per session. This authentication is browser-based. When a user enters a user name and password in their browser to authenticate with the explicit web proxy, this information is stored by the browser in a session cookie. Each new session started by the same web browser uses the session cookie for authentication. When the session cookie expires the user has to re-authenticate. If the user starts another browser on the same PC or closes and then re-opens their browser they have to authenticate again.

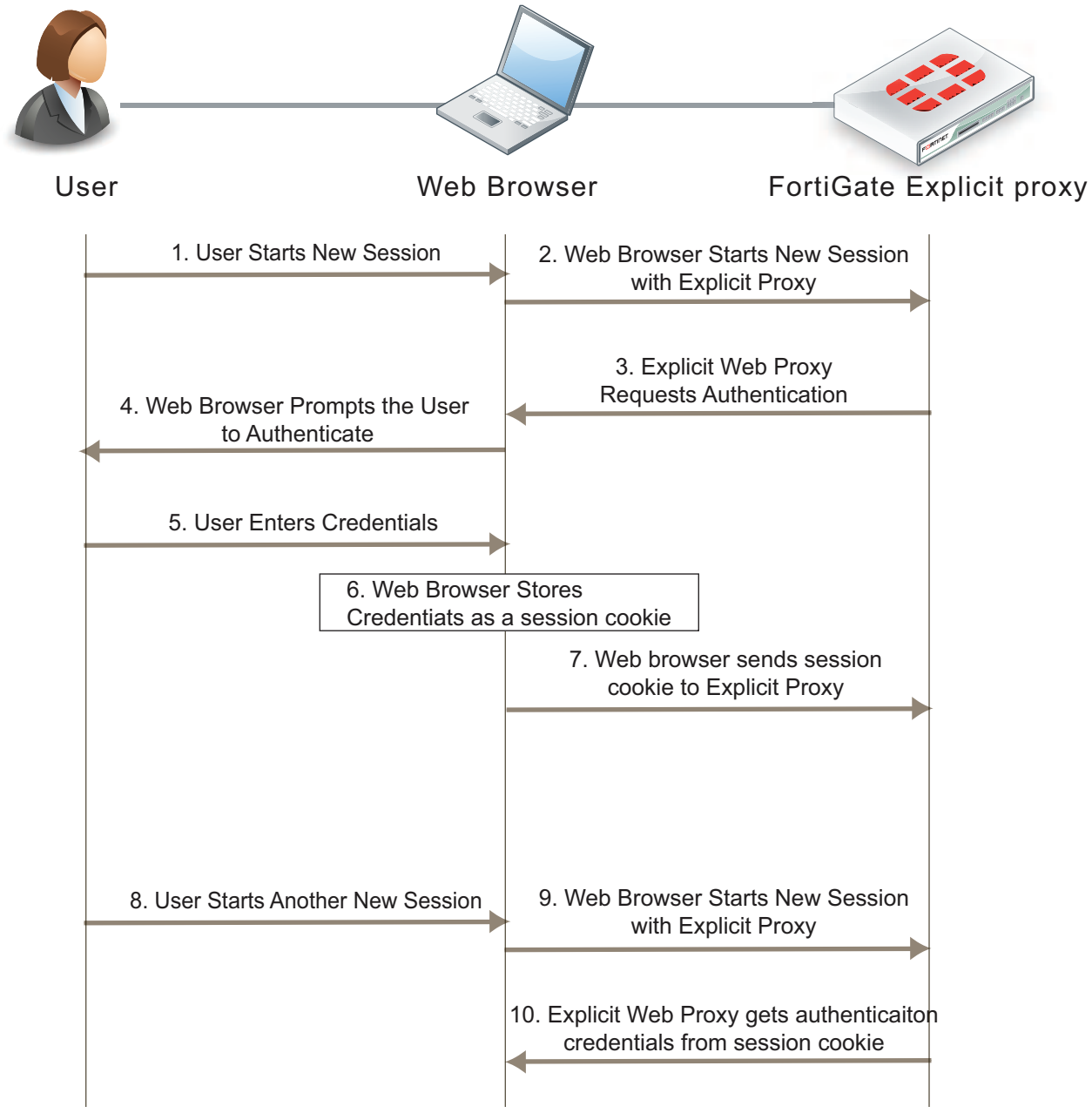
Since the authentication is browser-based, multiple clients with the same IP address can authenticate with the proxy using their own credentials. HTTP authentication provides authentication for multiple user sessions from the same source IP address. This can happen if there is a NAT device between the users and the FortiGate unit. HTTP authentication also supports authentication for other configurations that share one IP address among multiple users. These includes Citrix products and Windows Terminal Server and other similar virtualization solutions.

To configure per session authentication, add a explicit web proxy policy, set the **Action** to **AUTHENTICATE**, and make sure **Enable IP Based Authentication** is not selected.

Use the following CLI command to add per session authentication to a security policy. Per session authentication is selected by setting `ip-based` to `disable`.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set scraddr User_network
      set dstintf port1
      set dstaddr all
      set action accept
      set identity-based enable
      set ip-based disable
         config identity-based-policy
            edit 0
               set groups Internal_users
               set users dwhite rlee
               set schedule always
            end
   end
```

Per session HTTP authentication



Transaction-based authentication

Multiple HTTP transactions (request/response) may be pipelined in the same TCP connection. Typically, all HTTP transactions of a TCP connection are considered as belonging to the same user. However, some devices (e.g., load balancers) may send HTTP transactions of different users to the same TCP connection and to explicit proxy. In order to support this deployment case, transaction-based authentication can be implemented to require each HTTP transaction to be authenticated separately.

To implement transaction-based authentication in the CLI:

```
config firewall explicit-proxy-policy
   edit <id>
      set transaction-based enable
   next
end
```

Security profiles, threat weight, device identification, and the explicit web proxy

You can apply all security profiles to explicit web proxy sessions. This includes antivirus, web filtering, intrusion protection (IPS), application control, data leak prevention (DLP), and SSL/SSH inspection. Security profiles are applied by selecting them in an explicit web proxy policy or in authentication rules added to web proxy policies.

Traffic accepted by explicit web proxy policies contributes to threat weight data.

The explicit web proxy is not compatible with device identification.

Since the traffic accepted by the explicit web proxy is known to be either HTTP, HTTPS, or FTP over HTTP and since the ports are already known by the proxy, the explicit web proxy does not use all of the SSL/SSH inspection options. The explicit web proxy does support the following proxy options:

- Enable chunked bypass
- HTTP oversized file action and threshold

The explicit web proxy does not support the following proxy options:

- Client comforting
- Server comforting
- Monitor content information from dashboard. URLs visited by explicit web proxy users are not added to dashboard usage and log and archive statistics widgets.

For explicit web proxy sessions, the FortiGate unit applies antivirus scanning to HTTP POST requests and HTTP responses. The FortiGate unit starts virus scanning a file in an HTTP session when it receives a file in the body of an HTML request. The explicit web proxy can receive HTTP responses from either the originating web server or the FortiGate web cache module.

Web Proxy firewall services and service groups

Configure web proxy services by selecting **Explicit Proxy** when configuring a service. Web proxy services can be selected in a explicit web proxy policy when adding one from the CLI. If you add a policy from the web-based manager the service is set to the **webproxy** service. The webproxy service should be used in most cases, it matches with any traffic with any port number. However, if you have special requirements, such as using a custom protocol type or a reduced port range or need to add an IP/FQDN to an explicit proxy service you can create custom explicit web proxy services.

Web proxy services are similar to standard firewall services. You can configure web proxy services to define one or more protocols and port numbers that are associated with each web proxy service. Web proxy services can also be grouped into web proxy service groups.

One way in which web proxy services differ from firewall services is the protocol type you can select. The following protocol types are available:

- ALL
- CONNECT
- FTP

- HTTP
- SOCKS-TCP
- SOCKS-UDP

To add a web proxy service go to **Policy & Objects > Objects > Services** and select **Create New**. Set **Service Type** to **Explicit Proxy** and configure the service as required.

To add a web proxy service from the CLI enter:

```
config firewall service custom
   edit my-socks-service
      set explicit-proxy enable
      set category Web Proxy
      set protocol SOCKS-TCP
      set tcp-portrange 3450-3490
   end
```

To add a web proxy service group go to **Policy & Objects > Objects > Services** and select **Create New > Service Group**. Set **Type** to **Explicit Proxy** and add web proxy services to the group as required.

To add a web proxy service group from the CLI enter:

```
config firewall service group
   edit web-group
      set explicit-proxy enable
      set member webproxy my-socks-service
   end
```

Explicit web proxy firewall address URL patterns

You can add URL pattern addresses and address groups to control the destination URLs that explicit proxy users can connect to. To add a URL pattern to go to **Policy & Objects > Objects > Addresses**, select **Create New** and set the Type to **URL Pattern (Explicit Proxy)**. Add a URL or URL pattern that defines the URL or URLs that explicit proxy users should be limited to. Set the **Interface** to **any**.

For example to limit access to a single website:

www.fortinet.com

To limit access to websites from the same domain:

google.com

To limit access to a part of a website:

www.apple.com/ipad/

To add a URL pattern group, create several URL pattern addresses then go to **Policy & Objects > Objects > Addresses**, select **Create New > Group** and add URL patterns to the address group.

Then when creating explicit web proxy policies, select the URL pattern addresses or groups as the destination address.

URL patterns and HTTPS scanning

For HTTPS traffic, URL patterns can only be matched up to the root path. For example, consider the following URL pattern:

www.apple.com/ipad/

If a proxy user browses using HTTP, this URL pattern limits their access the iPad pages of www.apple.com. However, if a proxy user browses using HTTPS, they will be able to access all pages on www.apple.com.

Changing HTTP headers

You can create explicit web proxy profiles that can add, remove and change HTTP headers. The explicit web proxy profile can be added to a web explicit proxy policy and will be applied to all of the HTTP traffic accepted by that policy.

You can change the following HTTP headers:

- client-ip
- via header for forwarded requests
- via header for forwarded responses
- x-forwarded-for
- front-end-https

For each of these headers you can set the action to:

- Pass to forward the traffic without changing the header
- Add to add the header
- Remove to remove the header

You can also configure how the explicit web proxy handles custom headers. The proxy can add or remove custom headers from requests or responses. If you are adding a header you can specify the content to be included in the added header.

Create web proxy profiles from the CLI:

```
config web-proxy profile
   edit <name>
      set header-client-ip {add | pass | remove}
      set header-via-request {add | pass | remove}
      set header-via-response {add | pass | remove}
      set header-x-forwarded-for {add | pass | remove}
      set header-front-end-https {add | pass | remove}
         config headers
            edit <id>
               set action {add-to-request | add-to-response | remove-from-request |
                   remove-from-response}
               set content <string>
               set name <name>
            end
   end
```

Use the following command to add a web proxy profile to an explicit proxy policy:

```
config firewall explicit-proxy-policy
   edit <id>
      set webproxy-profile <name>
   end
```

Preventing the explicit web proxy from changing source addresses

By default in NAT/Route mode the explicit web proxy changes the source address of packets leaving the FortiGate to the IP address of the FortiGate interface that the packets are exiting from. In Transparent mode the

source address is changed to the management IP.

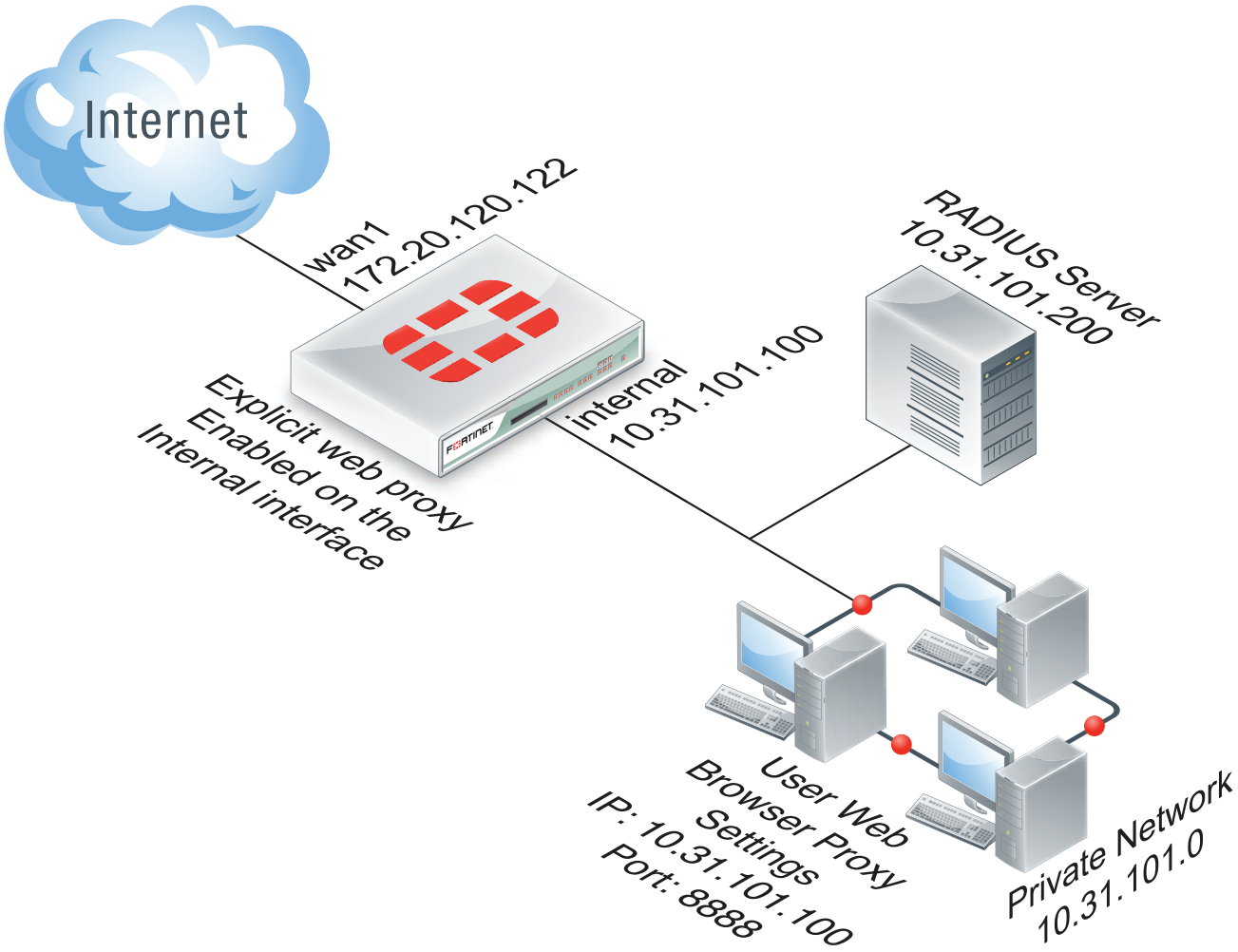
This configuration hides the IP addresses of clients and allows packets to return to the FortiGate unit interface without having to route packets from clients. You can use the following command to configure the explicit web proxy to keep the original client's source IP address:

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set transparent enable
   end
```

Example users on an internal network browsing the Internet through the explicit web proxy with web caching, RADIUS authentication, web filtering and virus scanning

This example describes how to configure the explicit web proxy for the example network shown below. In this example, users on the internal network connect to the explicit web proxy through the Internal interface of the FortiGate unit. The explicit web proxy is configured to use port 8888 so users must configure their web browser proxy settings to use port 8888 and IP address 10.31.101.100.

Example explicit web proxy network topology



Explicit web proxy users must authenticate with a RADIUS server before getting access to the proxy. The explicit proxy policy that accepts explicit web proxy traffic applies per session authentication and includes a RADIUS server user group. The authentication rule also applies web filtering and virus scanning.

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Enable the explicit web proxy for HTTP and HTTPS and change the HTTP and HTTPS ports to 8888.
2. Enable the explicit web proxy on the internal interface.
3. Add a RADIUS server and user group for the explicit web proxy.
4. Add an authentication explicit proxy policy. Enable web caching. Add an authentication rule and enable antivirus and web filtering.

Configuring the explicit web proxy - web-based manager

Use the following steps to configure the explicit web proxy.

To enable and configure the explicit web proxy

1. Go to **System > Config > Features** and turn on the **Explicit Proxy** feature.
2. Go to **System > Network > Explicit Proxy** and change the following settings:

Enable Explicit Web Proxy	Select **HTTP/HTTPS**.
Listen on Interfaces	No change. This field will eventually show that the explicit web proxy is enabled for the Internal interface.
HTTP Port	8888
HTTPS Port	0
Realm	You are authenticating with the explicit web proxy.
Default Firewall Policy Action	Deny

3. Select **Apply**.

To enable the explicit web proxy on the Internal interface

1. Go to **System > Network > Interfaces**.
2. Edit the internal interface.
3. Select **Enable Explicit Web Proxy.**
4. Select **OK**.

To add a RADIUS server and user group for the explicit web proxy

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New** to add a new RADIUS server:

Name	RADIUS_1
Primary Server Name/IP	10.31.101.200
Primary Server Secret	RADIUS_server_secret

2. Select **OK**.
3. Go to **User & Device > User > User Groups** and select **Create New** to add a new user group.

Name	Explict_proxy_user_group
Type	Firewall
Remote Groups	RADIUS_1
Group Name	Any

4. Select **OK**.

To add an explicit proxy policy

1. Go to **Policy & Objects > Objects > Addresses** and select **Create New**.
2. Add a firewall address for the internal network:

Category	Address
Name	Internal_subnet
Type	Subnet / IP Range
Subnet / IP Range	10.31.101.0
Interface	Any

3. Go to **Policy & Objects > Policy > Explicit Proxy** and select **Create New**.
4. Configure the explicit web proxy policy.

Explicit Proxy Type	Web
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	all
Action	AUTHENTICATE

5. Under **Configure Authentication Rules** select **Create New** to add an authentication rule:

Groups	Explicit_policy

Source User(s)	Leave blank
Schedule	always

6. Turn on **Antivirus** and **Web Filter** and select the **default** profiles for both.
7. Select the **default** proxy options profile.
8. Select **OK**.
9. Make sure **Enable IP Based Authentication** is not selected.
10. Turn on **Web Cache**.
11. Select **OK**.

Configuring the explicit web proxy - CLI

Use the following steps to configure the example explicit web proxy configuration from the CLI.

To enable the explicit web proxy on the Internal interface

1. Enter the following command to enable the explicit web proxy on the internal interface.

```
config system interface
   edit internal
      set explicit-web-proxy enable
end
```

To enable and configure the explicit web proxy

1. Enter the following command to enable the explicit web proxy and set the TCP port that proxy accepts HTTP and HTTPS connections on to 8888.

```
config web-proxy explicit
   set status enable
   set http-incoming-port 8888
   set https-incoming-port 8888
   set realm "You are authenticating with the explicit web proxy"
   set sec-default-action deny
end
```

To add a RADIUS server and user group for the explicit web proxy

1. Enter the following command to add a RADIUS server:

```
config user radius
   edit RADIUS_1
      set server 10.31.101.200
      set secret RADIUS_server_secret
end
```

2. Enter the following command to add a user group for the RADIUS server.

```
config user group
   edit Explicit_proxy_user_group
      set group-type firewall
      set member RADIUS_1
end
```

To add a security policy for the explicit web proxy

1. Enter the following command to add a firewall address for the internal subnet:

```
config firewall address
   edit Internal_subnet
      set type iprange
      set start-ip 10.31.101.1
      set end-ip 10.31.101.255
end
```

2. Enter the following command to add the explicit web proxy security policy:

```
config firewall explicit-proxy-policy
   edit 0
      set proxy web
      set dstintf wan1
      set srcaddr Internal_subnet
      set dstaddr all
      set action accept
      set service webproxy
      set webcache enable
      set identity-based enable
      set ipbased disable
      set active-auth-method basic
         config identity-based-policy
            edit 0
               set groups Explicit_Proxy_user_group
               set schedule always
               set utm-status enable
               set av-profile default
               set webfilter-profile default
               set profile-protocol-options default
            end
end
```

Testing and troubleshooting the configuration

You can use the following steps to verify that the explicit web proxy configuration is working as expected:

To test the explicit web proxy configuration

1. Configure a web browser on the internal subnet to use a web proxy server at IP address 10.31.101.100 and port 8888.
2. Browse to an Internet web page.
   The web browser should pop up an authentication window that includes the phrase that you added to the Realm option.
3. Enter the username and password for an account on the RADIUS server.
   If the account is valid you should be allowed to browse web pages on the Internet.
4. Close the browser and clear its cache and cookies.
5. Restart the browser and connect to the Internet.
   You could also start a second web browser on the same PC. Or you could start a new instance of the same browser as long as the browser asks for a user name and password again.

   You should have to authenticate again because identity-based policies are set to session-based authentication.

6. If this basic functionality does not work, check your FortiGate and web browser configuration settings.
7. Browse to a URL on the URL filter list and confirm that the web page is blocked.
8. Browse to http://eicar.org and attempt to download an anti-malware test file.
   The antivirus configuration should block the file.
   Sessions for web-proxy security policies do not appear on the Top Sessions dashboard widget and the count column for security policies does not display a count for explicit web proxy security policies.
9. You can use the following command to display explicit web proxy sessions

```
get test wad 60
IP based users:

Session based users:
   user:0x9c20778, username:User1, vf_id:0, ref_cnt:9

Total allocated user:1

Total user count:3, shared user quota:50, shared user count:3
```

   This command output shows one explicit proxy user with user name `User1` authenticated using session-based authentication.

Explicit web proxy sessions and user limits

Web browsers and web servers open and close multiple sessions with the explicit web proxy. Some sessions open and close very quickly. HTTP 1.1 keepalive sessions are persistent and can remain open for long periods of time. Sessions can remain on the explicit web proxy session list after a user has stopped using the proxy (and has, for example, closed their browser). If an explicit web proxy session is idle for more than 3600 seconds it is torn down by the explicit web proxy. See RFC 2616 for information about HTTP keepalive/persistent HTTP sessions.

This section describes proxy sessions and user limits for both the explicit web proxy and the explicit FTP proxy. Session and user limits for the two proxies are counted and calculated together. However, in most cases if both proxies are active there will be many more web proxy sessions than FTP proxy sessions.

The FortiGate unit adds two sessions to its session table for every explicit proxy session started by a web browser and every FTP session started by an FTP client. An entry is added to the session table for the session from the web browser or client to the explicit proxy. All of these sessions have the same destination port as the explicit web proxy port (usually 8080 for HTTP and 21 for FTP). An entry is also added to the session table for the session between the exiting FortiGate interface and the web or FTP server destination of the session. All of these sessions have a FortiGate interface IP address and the source address of the session and usually have a destination port of 80 for HTTP and 21 for FTP.

Proxy sessions that appear in FortiView do not include the Policy ID of the web-proxy or ftp-proxy security policy that accepted them. However, the explicit proxy sessions include a destination port that matches the explicit proxy port number (usually 8080 for the web proxy and 21 for the FTP proxy). The proxied sessions from the FortiGate unit have their source address set to the IP address of the FortiGate unit interface that the sessions use to connect to their destinations (for example, for connections to the Internet the source address would be the IP address of the FortiGate interface connected to the Internet).

FortiOS limits the number of explicit proxy users. This includes both explicit FTP proxy and explicit web proxy users. The number of users varies by FortiGate model from as low as 10 to up to 18000 for high end models. You cannot raise this limit.

If your FortiGate unit is configured for multiple VDOMs you can go to **System > VDOM > Global Resources** to view the maximum number of **Concurrent explicit proxy users** and optionally reduce the limit. You can also use the following command:

```
config global
   config system resource-limits
      set proxy 50
   end
end
```

To limit the number of explicit proxy users for a VDOM, from the web-based manager enable multiple VDOMs and go to **System > VDOM > VDOM** and edit a VDOM or use the following command to change the number of explicit web proxy users for VDOM_1:

```
config global
   config system vdom-property
      edit VDOM_1
         set proxy 25
   end
end
```

You can use the `diagnose wad user list` command to view the number of explicit web proxy users. Users may be displayed with this command even if they are no longer actively using the proxy. All idle sessions time out after 3600 seconds.

You can use the command `diagnose wad user clear` to clear current explicit proxy users. You can also use the command `diagnose wad user clear <user-name>` to clear individual users. This means delete information about all users and force them re-authenticate.

Users that authenticate with explicit web-proxy or ftp-proxy security policies do not appear in the **User & Device > Monitor > Firewall** list and selecting **De-authenticate All Users** has no effect on explicit proxy users.

How the number of concurrent explicit proxy users is determined depends on their authentication method:

- For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LADAP, FSAE, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user.
- For IP Based authentication, or no authentication, or if no web-proxy security policy has been added, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.

The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

The FortiGate explicit FTP proxy

You can use the FortiGate explicit FTP proxy to enable explicit FTP proxying on one or more FortiGate interfaces. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiGate interfaces.

Explicit FTP proxies are configured for each VDOM when multiple VDOMs are enabled.

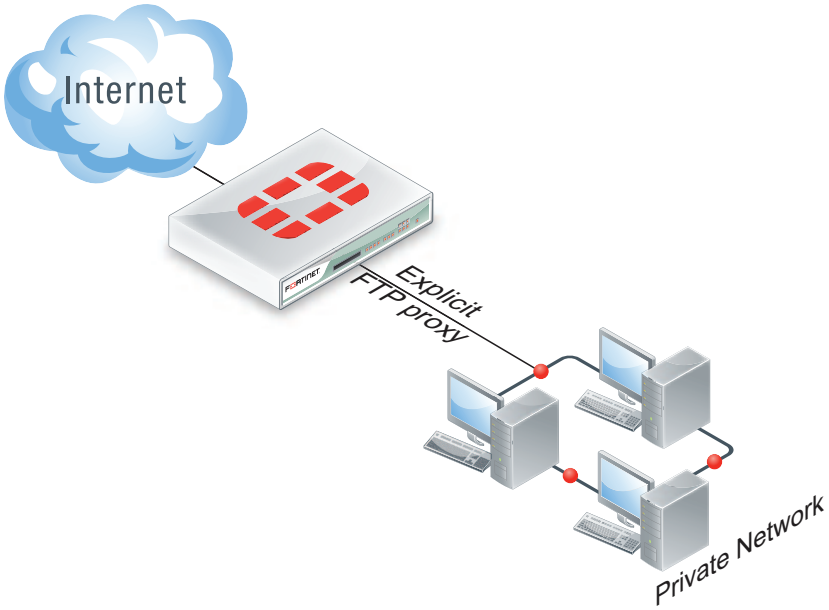
In most cases you would configure the explicit FTP proxy for users on a network by enabling the explicit FTP proxy on the FortiGate interface connected to that network. Users on the network would connect to and authenticate with the explicit FTP proxy before connecting to an FTP server. In this case the IP address of the explicit FTP proxy is the IP address of the FortiGate interface on which the explicit FTP proxy is enabled.

Enabling the explicit FTP proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

If the FortiGate unit is operating in Transparent mode, users would configure their browsers to use a proxy server with the FortiGate unit management IP address.

The FTP proxy receives FTP sessions to be proxied at FortiGate interfaces with the explicit FTP proxy enabled. The FTP proxy uses FortiGate routing to route sessions through the FortiGate unit to a destination interface. Before a session leaves the exiting interface, the explicit FTP proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the FortiGate unit is operating in Transparent mode the explicit web proxy changes the source addresses to the management IP address.

Example explicit FTP proxy topology



To allow anyone to anonymously log into explicit FTP proxy and connect to any FTP server you can set the explicit FTP proxy default firewall proxy action to accept. When you do this, users can log into the explicit FTP proxy with any username and password.

In most cases you would want to use explicit proxy policies to control explicit FTP proxy traffic and apply security features, access control/authentication, and logging. You can do this by keeping the default explicit FTP proxy firewall policy action to deny and then adding explicit FTP proxy policies. In most cases you would also want users to authenticate with the explicit FTP proxy. By default an anonymous FTP login is required. Usually you would add authentication to explicit FTP proxy policies. Users can then authenticate with the explicit FTP proxy according to users or user groups added to the policies. User groups added to explicit FTP proxy policies can use any authentication method supported by FortiOS including the local user database and RADIUS and other remote servers.

If you leave the default firewall policy action set to deny and add explicit FTP proxy policies, all connections to the explicit FTP proxy must match an or else they will be dropped. Sessions that are accepted are processed according to the ftp-proxy security policy settings.

You can also change the explicit FTP proxy default firewall policy action to accept and add explicit FTP proxy policies. If you do this, sessions that match explicit FTP proxy policies are processed according to the policy settings. Connections to the explicit FTP proxy that do not match an explicit FTP proxy policy are allowed and the users can authenticate with the proxy anonymously.

There are some limitations to the security features that can be applied to explicit FTP proxy sessions. See Security profiles, threat weight, device identification, and the explicit FTP proxy on page 2929.

You cannot configure IPsec, SSL VPN, or Traffic shaping for explicit FTP proxy traffic. Explicit FTP proxy policies can only include firewall addresses not assigned to a FortiGate unit interface or with interface set to **any**. (On the web-based manager you must set the interface to **Any**. In the CLI you must `unset` the `associated-interface`.)

How to use the explicit FTP proxy to connect to an FTP server

To connect to an FTP server using the explicit FTP proxy, users must run an FTP client and connect to the IP address of a FortiGate interface on which the explicit FTP proxy is enabled. This connection attempt must use the configured explicit FTP proxy port number (default 21).

The explicit FTP proxy is not compatible with using a web browser as an FTP client. To use web browsers as FTP clients configure the explicit web proxy to accept FTP sessions.

The following steps occur when a user starts an FTP client to connect to an FTP server using the explicit FTP proxy. Any RFC-compliant FTP client can be used. This example describes using a command-line FTP client. Some FTP clients may require a custom FTP proxy connection script.

1. The user enters a command on the FTP client to connect to the explicit FTP proxy.

   For example, if the IP address of the FortiGate interface on which the explicit FTP proxy is enabled is 10.31.101.100, enter:

   ```
   ftp 10.31.101.100
   ```

2. The explicit FTP proxy responds with a welcome message and requests the user's FTP proxy user name and password and a username and address of the FTP server to connect to:

   ```
   Connected to 10.31.101.100.
   220 Welcome to Fortigate FTP proxy
   Name (10.31.101.100:user):
   ```

   You can change the message by editing the FTP Explicit Banner Message replacement message.

3. At the prompt the user enters their FTP proxy username and password and a username and address for the FTP server. The FTP server address can be a domain name or numeric IP address. This information is entered using the following syntax:

   ```
   <proxy-user>:<proxy-password>:<server-user>@<server-address>
   ```

   For example, if the proxy username and password are `p-name` and `p-pass` and a valid username for the FTP server is `s-name` and the server's IP address is `ftp.example.com` the syntax would be:

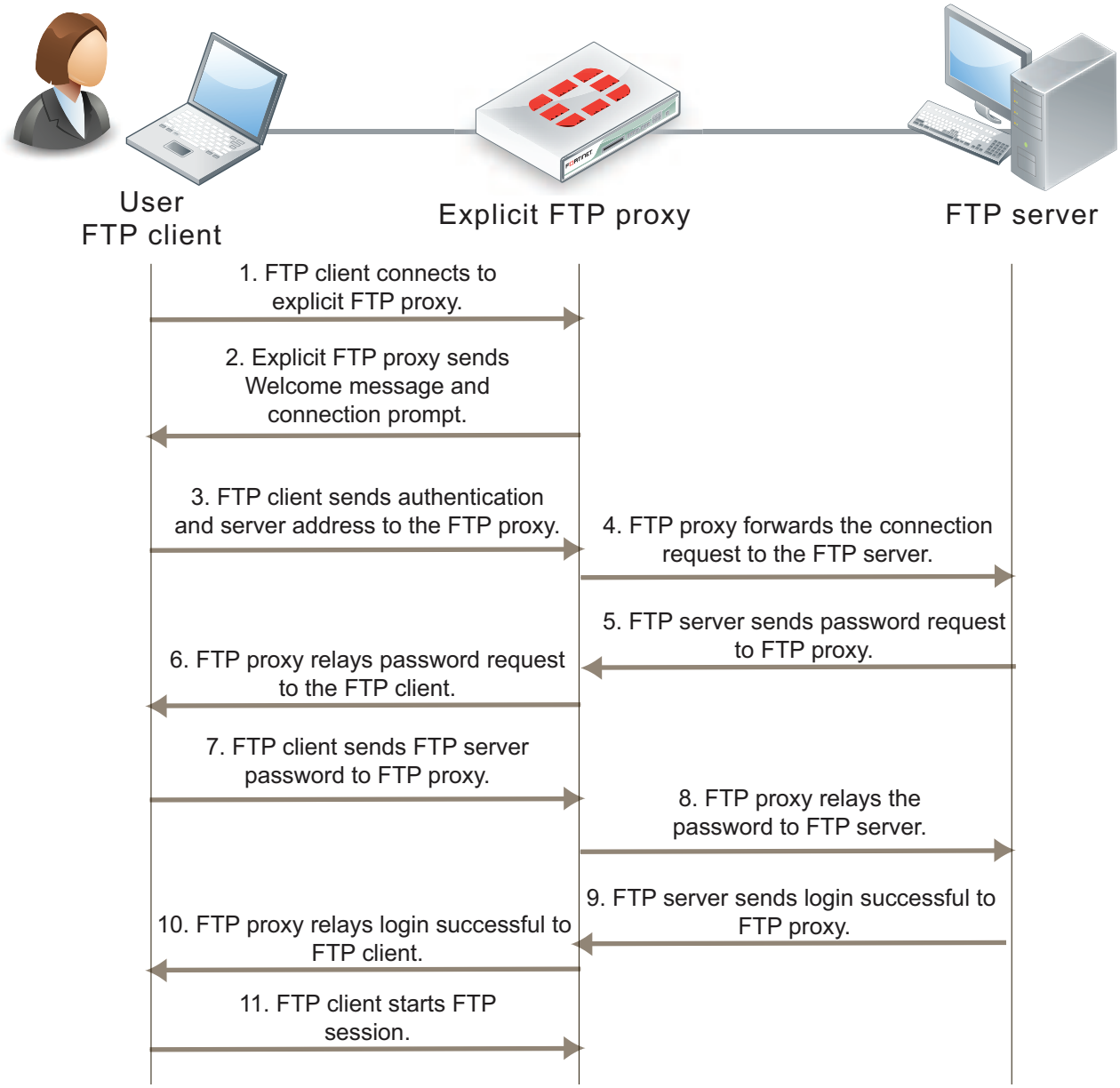
   ```
   p-name:p-pass:s-name@ftp.example.com
   ```

If the FTP proxy accepts anonymous logins `p-name` and `p-pass` can be any characters.

4. The FTP proxy forwards the connection request, including the user name, to the FTP server.
5. If the user name is valid for the FTP server it responds with a password request prompt.
6. The FTP proxy relays the password request to the FTP client.
7. The user enters the FTP server password and the client sends the password to the FTP proxy.
8. The FTP proxy relays the password to the FTP server.
9. The FTP server sends a login successful message to the FTP proxy.
10. The FTP proxy relays the login successful message to the FTP client.
11. The FTP client starts the FTP session.

    All commands entered by the client are relayed by the proxy to the server. Replies from the server are relayed back to the FTP client.

Explicit FTP proxy session



From a simple command line FTP client connecting to an the previous sequence could appear as follows:

```
ftp 10.31.101.100 21
Connected to 10.31.101.100.
220 Welcome to Fortigate FTP proxy
Name (10.31.101.100:user): p-name:p-pass:s-name@ftp.example.com
331 Please specify the password.
Password: s-pass
230 Login successful.
Remote system type is UNIX
Using binary mode to transfer files.
ftp>
```

General explicit FTP proxy configuration steps

You can use the following general steps to configure the explicit FTP proxy.

To enable the explicit FTP proxy - web-based manager:

1. Go to **System > Network > Explicit Proxy > Explicit FTP Proxy Options**. Select **Enable Explicit FTP Proxy** to turn on the explicit FTP proxy.
2. Select Apply.

   The **Default Firewall Policy Action** is set to **Deny** and requires you to add a explicit FTP proxy policy to allow access to the explicit FTP proxy. This configuration is recommended and is a best practice because you can use policies to control access to the explicit FTP proxy and also apply security features and authentication.
3. Go to **System > Network > Interface** and select one or more interfaces for which to enable the explicit web proxy. Edit the interface and select **Enable Explicit FTP Proxy**.

Enabling the explicit FTP proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address. If you enable the proxy on such an interface make sure authentication is required to use the proxy.

4. Go to **Policy & Objects > Policy > Explicit Proxy** and select **Create New** and set the **Explicit Proxy Type** to **FTP.**

   You can add multiple explicit FTP proxy policies.
5. Configure the policy as required to accept the traffic that you want to be processed by the explicit FTP proxy.

   The source address of the policy should match client source IP addresses. The firewall address selected as the source address cannot be assigned to a FortiGate interface. The Interface field of the firewall address must be blank or it must be set to **Any**.

   The destination address of the policy should match the IP addresses of FTP servers that clients are connecting to. The destination address could be **all** to allow connections to any FTP server.

   If **Default Firewall Policy Action** is set to Deny, traffic sent to the explicit FTP proxy that is not accepted by an explicit FTP proxy policy is dropped. If **Default Firewall Policy Action** is set to Allow then all FTP proxy sessions that don't match a policy are allowed.

   For example the following explicit FTP proxy policy allows users on an internal network to access FTP servers on the Internet through the wan1 interface of a FortiGate unit.

Explicit Proxy Type	FTP
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	all

Schedule	always
Action	ACCEPT

The following explicit FTP proxy policy requires users on an internal network to authenticate with the FortiGate unit before accessing FTP servers on the Internet through the wan1 interface.

Explicit Proxy Type	FTP
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	all
Action	AUTHENTICATE

6. Select **Create New** to add an **Authentication Rule** and configure the rule as follows:

Groups	Proxy-Group
Source Users	(optional)
Schedule	always

7. Add security profiles as required and select **OK**.
8. You can add multiple authentication rules to apply different authentication for different user groups and users and also apply different security profiles and logging settings for different users.
9. Select **OK**.

To enable the explicit FTP proxy - CLI:

1. Enter the following command to turn on the explicit FTP proxy. This command also changes the explicit FTP proxy port to 2121.

```
config ftp-proxy explicit
   set status enable
   set incoming-port 2121
end
```

The default explicit FTP proxy configuration has `sec-default-action` set to `deny` and requires you to add a security policy to allow access to the explicit FTP proxy.

2. Enter the following command to enable the explicit FTP proxy for the internal interface.

```
config system interface
   edit internal
      set explicit-ftp-proxy enable
   end
end
```

3. Use the following command to add a firewall address that matches the source address of users who connect to the explicit FTP proxy.

```
config firewall address
   edit Internal_subnet
      set type iprange
```

```
      set start-ip 10.31.101.1
      set end-ip 10.31.101.255
   end
```

The source address for a ftp-proxy security policy cannot be assigned to a FortiGate unit interface.

4. Use the following command to add an explicit FTP proxy policy that allows all users on the internal subnet to use the explicit FTP proxy for connections through the wan1 interface to the Internet.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy ftp
      set dstintf wan1
      set scraddr Internal_subnet
      set dstaddr all
      set action accept
      set schedule always
end
```

5. Use the following command to add an explicit FTP proxy policy that allows authenticated users on the internal subnet to use the explicit FTP proxy for connections through the wan1 interface to the Internet.

```
config firewall explicit-proxy-policy
   edit 0
      set proxy ftp
      set dstintf wan1
      set scraddr Internal_subnet
      set dstaddr Fortinet-web-sites
      set action accept
      set schedule always
      set identity-based enable
         config identity-based-policy
            edit 1
               set groups Proxy-group
               set schedule always
 end
end
```

Restricting the IP address of the explicit FTP proxy

You can use the following command to restrict access to the explicit FTP proxy using only one IP address. The IP address that you specify must be the IP address of an interface that the explicit FTP proxy is enabled on. You might want to use this option if the explicit FTP proxy is enabled on an interface with multiple IP addresses.

For example, to require uses to connect to the IP address 10.31.101.100 to connect to the explicit FTP proxy:

```
config ftp-proxy explicit
   set incoming-ip 10.31.101.100
end
```

Restricting the outgoing source IP address of the explicit FTP proxy

You can use the following command to restrict the source address of outgoing FTP proxy packets to a single IP address. The IP address that you specify must be the IP address of an interface that the explicit FTP proxy is enabled on. You might want to use this option if the explicit FTP proxy is enabled on an interface with multiple IP addresses.

For example, to restrict the outgoing packet source address to 172.20.120.100:

```
config ftp-proxy explicit
   set outgoing-ip 172.20.120.100
end
```

Security profiles, threat weight, device identification, and the explicit FTP proxy

You can apply antivirus, data leak prevention (DLP), and SSL/SSH inspection to explicit FTP proxy sessions. Security profiles are applied by selecting them in an explicit FTP proxy policy or an authentication rule in an FTP proxy security policy.

Traffic accepted by explicit FTP proxy policies contributes to threat weight data.

The explicit FTP proxy is not compatible with device identification.

Explicit FTP proxy options and SSL/SSH inspection

Since the traffic accepted by the explicit FTP proxy is known to be FTP and since the ports are already known by the proxy, the explicit FTP proxy does not use the FTP port proxy options settings.

When adding UTM features to an FTP proxy security policy, you must select a proxy options profile. In most cases you can select the default proxy options profile. You could also create a custom proxy options profile.

The explicit FTP proxy supports the following proxy options:

- Block Oversized File and oversized file limit

The explicit FTP proxy does not support the following protocol options:

- Client comforting

Explicit FTP proxy sessions and antivirus

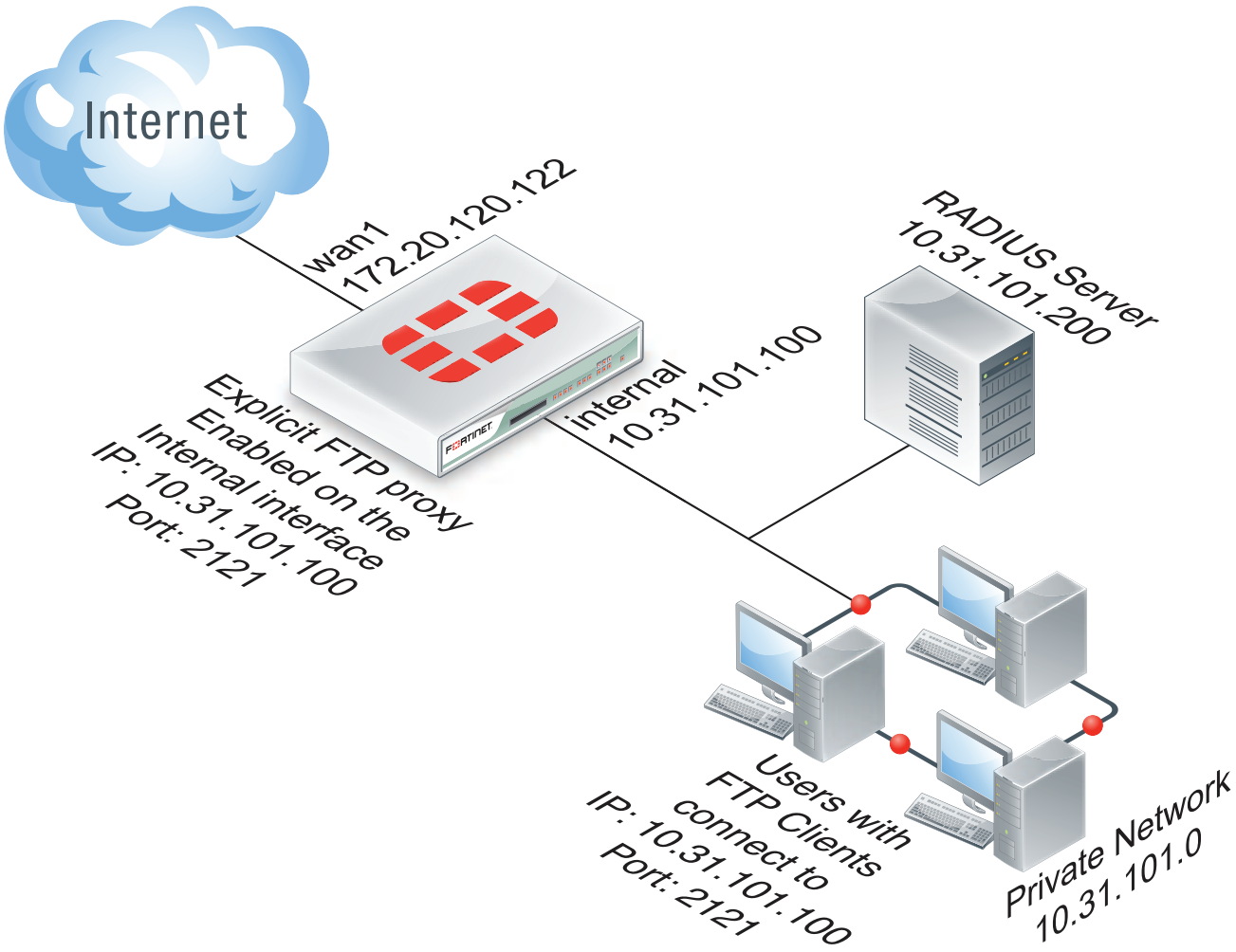
For explicit FTP proxy sessions, the FortiGate unit applies antivirus scanning to FTP file GET and PUT requests. The FortiGate unit starts virus scanning a file in an FTP session when it receives a file in the body of an FTP request.

Flow-based virus scanning is not available for explicit FTP proxy sessions. Even if the FortiGate unit is configured to use flow-based antivirus, explicit FTP proxy sessions use the regular virus database.

Example users on an internal network connecting to FTP servers on the Internet through the explicit FTP with RADIUS authentication and virus scanning

This example describes how to configure the explicit FTP proxy for the example network shown below. In this example, users on the internal network connect to the explicit FTP proxy through the Internal interface with IP address 10.31.101.100. The explicit web proxy is configured to use port 2121 so to connect to an FTP server on the Internet users must first connect to the explicit FTP proxy using IP address 10.31.101.100 and port 2121.

Example explicit FTP proxy network topology



In this example, explicit FTP proxy users must authenticate with a RADIUS server before getting access to the proxy. To apply authentication, the security policy that accepts explicit FTP proxy traffic includes an identity based policy that applies per session authentication to explicit FTP proxy users and includes a user group with the RADIUS server in it. The identity based policy also applies UTM virus scanning and DLP.

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Enable the explicit FTP proxy and change the FTP port to 2121.
2. Enable the explicit FTP proxy on the internal interface.
3. Add a RADIUS server and user group for the explicit FTP proxy.
4. Add a user identity security policy for the explicit FTP proxy.
5. Enable antivirus and DLP features for the identity-based policy.

Configuring the explicit FTP proxy - web-based manager

Use the following steps to configure the explicit FTP proxy from FortiGate web-based manager.

To enable and configure the explicit FTP proxy

1. Go to **System > Network > Explicit Proxy > Explicit FTP Proxy Options** and change the following settings:

Enable Explicit FTP Proxy	Select.
Listen on Interface	No change. This field will eventually show that the explicit web proxy is enabled for the Internal interface.
FTP Port	2121
Default Firewall Policy Action	Deny

2. Select **Apply**.

To enable the explicit FTP proxy on the Internal interface

1. Go to **System > Network > Interface**, edit the Internal interface and select **Enable Explicit FTP Proxy**.

To add a RADIUS server and user group for the explicit FTP proxy

1. Go to **User & Device > Authentication > RADIUS Servers**.
2. Select **Create New** to add a new RADIUS server:

Name	RADIUS_1
Primary Server Name/IP	10.31.101.200
Primary Server Secret	RADIUS_server_secret

3. Go to **User > User > User Groups** and select **Create New**.

Name	Explict_proxy_user_group
Type	Firewall
Remote groups	RADIUS_1
Group Name	ANY

4. Select **OK**.

To add a security policy for the explicit FTP proxy

1. Go to **Policy &Objects > Objects > Addresses** and select **Create New**.
2. Add a firewall address for the internal network:

Address Name	Internal_subnet
Type	Subnet
Subnet / IP Range	10.31.101.0
Interface	Any

3. Go to **Policy & Objects > Policy > Explicit Proxy** and select **Create New**.
4. Configure the explicit FTP proxy security policy.

Explicit Proxy Type	FTP
Source Address	Internal_subnet
Outgoing Interface	wan1
Destination Address	all
Action	AUTHENTICATE

5. Under **Configure Authentication Rules** select **Create New** to add an authentication rule:

Groups	Explicit_policy
Users	Leave blank
Schedule	always

6. Turn on **Antivirus** and **Web Filter** and select the **default** profiles for both.
7. Select the **default** proxy options profile.
8. Select **OK**.
9. Make sure **Enable IP Based Authentication** is not selected and **Default Authentication Method** is set to **Basic**.
10. Select **OK**.

Configuring the explicit FTP proxy - CLI

Use the following steps to configure the example explicit web proxy configuration from the CLI.

To enable and configure the explicit FTP proxy

1. Enter the following command to enable the explicit FTP proxy and set the TCP port that proxy accepts FTP connections on to 2121.

```
config ftp-proxy explicit
   set status enable
   set incoming-port 2121
   set sec-default-action deny
end
```

To enable the explicit FTP proxy on the Internal interface

1. Enter the following command to enable the explicit FTP proxy on the internal interface.

```
config system interface
   edit internal
      set explicit-ftp-proxy enable
end
```

To add a RADIUS server and user group for the explicit FTP proxy

1. Enter the following command to add a RADIUS server:

```
config user radius
   edit RADIUS_1
      set server 10.31.101.200
      set secret RADIUS_server_secret
end
```

2. Enter the following command to add a user group for the RADIUS server.

```
config user group
   edit Explicit_proxy_user_group
      set group-type firewall
      set member RADIUS_1
end
```

To add a security policy for the explicit FTP proxy

1. Enter the following command to add a firewall address for the internal subnet:

```
config firewall address
   edit Internal_subnet
      set type iprange
      set start-ip 10.31.101.1
      set end-ip 10.31.101.255
end
```

2. Enter the following command to add the explicit FTP proxy security policy:

```
config firewall explicit-proxy-policy
   edit 0
      set proxy ftp
      set dstintf wan1
      set srcaddr Internal_subnet
      set dstaddr all
      set action accept
      set identity-based enable
      set ipbased disable
      set active-auth-method basic
         config identity-based-policy
            edit 0
               set groups Explicit_Proxy_user_group
               set schedule always
               set utm-status enable
               set av-profile default
               set profile-protocol-options default
            end
   end
```

Testing and troubleshooting the configuration

You can use the following steps to verify that the explicit FTP proxy configuration is working as expected. These steps use a command line FTP client.

To test the explicit web proxy configuration

1. From a system on the internal network start an FTP client and enter the following command to connect to the FTP proxy:

   ```
   ftp 10.31.101.100
   ```

   The explicit FTP proxy should respond with a message similar to the following:

   ```
   Connected to 10.31.101.100.
   220 Welcome to Fortigate FTP proxy
   Name (10.31.101.100:user):
   ```

2. At the prompt enter a valid username and password for the RADIUS server followed by a user name for an FTP server on the Internet and the address of the FTP server. For example, if a valid username and password on the RADIUS server is ex_name and ex_pass and you attempt to connect to an FTP server at ftp.example.com with user name s_name, enter the following at the prompt:

   ```
   Name (10.31.101.100:user):ex_name:ex_pass:s_name@ftp.example.com
   ```

3. You should be prompted for the password for the account on the FTP server.
4. Enter the password and you should be able to connect to the FTP server.
5. Attempt to explore the FTP server file system and download or upload files.
6. To test UTM functionality, attempt to upload or download an ECAR test file. Or upload or download a tex file containing text that would be matched by the DLP sensor.

   For eicar test files, go to http://eicar.org.

Explicit FTP proxy sessions and user limits

FTP clients do not open large numbers of sessions with the explicit FTP proxy. Most sessions stay open for a short while depending on how long a user is connected to an FTP server and how large the file uploads or downloads are. So unless you have large numbers of FTP users, the explicit FTP proxy should not be adding large numbers of sessions to the session table.

Explicit FTP proxy sessions and user limits are combined with explicit web proxy session and user limits. For information about explicit proxy session and user limits, see Explicit web proxy sessions and user limits on page 2920.

FortiGate WCCP

The Web Cache Communication Protocol (WCCP) can be used to provide web caching with load balancing and fault tolerance. In a WCCP configuration, a WCCP server receives HTTP requests from user's web browsers and redirects the requests to one or more WCCP clients. The clients either return cached content or request new content from the destination web servers before caching it and returning it to the server which in turn returns the content to the original requestor. If a WCCP configuration includes multiple WCCP clients, the WCCP server load balances traffic among the clients and can detect when a client fails and failover sessions to still operating clients. WCCP is described by the Web Cache Communication Protocol Internet draft.

The sessions that are cached by WCCP depend on the configuration of the WCCP clients. If the client is a FortiGate unit, you can configure the port numbers and protocol number of the sessions to be cached. For example, to cache HTTPS traffic on port 443 the WCCP client port must be set to 443 and protocol must be set to 6. If the WCCP client should also cache HTTPS traffic on port 993 the client ports option should include both port 443 and 993.

On a FortiGate unit, WCCP sessions are accepted by a security policy before being cached. If the security policy that accepts sessions that do not match the port and protocol settings in the WCCP clients the traffic is dropped.

WCCP is configured per-VDOM. A single VDOM can operate as a WCCP server or client (not both at the same time). FortiGate units are compatible with third-party WCCP clients and servers. If a FortiGate unit is operating as an Internet firewall for a private network, you can configure it to cache and serve some or all of the web traffic on the private network using WCCP by adding one or more WCCP clients, configuring WCCP server settings on the FortiGate unit and adding WCCP security policies that accept HTTP session from the private network.

FortiGate units support WCCPv1 and WCCPv2. A FortiGate unit in NAT/Route or transparent mode can operate as a WCCP server. To operate as a WCCP client a FortiGate unit must be in NAT/Route mode. FortiGate units communicate between WCCP servers and clients over UDP port 2048. This communication can be encapsulated in a GRE tunnel or just use layer 2 forwarding.

A WCCP server can also be called a WCCP router. A WCCP client can also be called a WCCP cache engine.

WCCP service groups, service numbers, service IDs and well known services

A FortiGate unit configured as a WCCP server or client can include multiple server or client configurations. Each of these configurations is called a WCCP service group. A service group consists of one or more WCCP servers (or routers) and one or more WCCP clients working together to cache a specific type of traffic. The service group configuration includes information about the type of traffic to be cached, the addresses of the WCCP clients and servers and other information about the service.

A service group is identified with a numeric WCCP service ID (or service number) in the range 0 to 255. All of the servers and clients in the same WCCP service group must have service group configurations with the same WCCP service ID.

The value of the service ID provides some information about the type of traffic to be cached by the service group. Service IDs in the range 0 to 50 are reserved for well known services. A well known service is any service that is

defined by the WCCP standard as being well known. Since the service is well known, just the service ID is required to identify the traffic to be cached.

Even though the well known service ID range is 0 to 50, at this time only one well known service has been defined. Its service ID 0, which is used for caching HTTP (web) traffic.

So to configure WCCP to cache HTTP sessions you can add a service group to the WCCP router and WCCP clients with a service ID of 0. No other information about the type of traffic to cache needs to be added to the service group.

Since service IDs 1 to 50 are reserved for well know services and since these services are not defined yet, you should not add service groups with IDs in the range 1 to 50.

FortiOS does allow you to add service groups with IDs between 1 and 50. Since these service groups have not been assigned well known services, however, they will not cache any sessions. Service groups with IDs 51 to 255 allow you to set the port numbers and protocol number of the traffic to be cached. So you can use service groups with IDs 51 to 255 to cache different kinds of traffic based on port numbers and protocol number of the traffic. Service groups 1 to 50; however, do not allow you to set port numbers or protocol numbers so cannot be used to cache any traffic.

To cache traffic other than HTTP traffic you must add service groups with IDs in the range 51 to 255. These service group configurations must include the port numbers and protocol number of the traffic to be cached. It is the port and protocol number configuration in the service group that determines what traffic will be cached by WCCP.

Example WCCP server and client configuration for caching HTTP sessions (service ID = 0)

Enter the following command to add a WCCP service group to a WCCP server that caches HTTP sessions. The IP address of the server is 10.31.101.100 and the WCCP clients are on the 10.31.101.0 subnet. The service

ID of this service group is 0.

```
config system wccp
   edit 0
      set router-id 10.31.101.100
      set server-list 10.31.101.0 255.255.255.0
   end
```

Enter the following commands to configure a FortiGate unit to operate as a WCCP client and add a service group that configures the client to cache HTTP sessions. The IP address of the server is 10.31.101.100 and IP address of this WCCP clients is 10.31.101.1 subnet. The service ID of this service group is 0.

```
config system settings
   set wccp-cache-engine enable
end

config system wccp
   edit 0
      set cache-id 10.31.101.1
      set router-list 10.31.101.100
   end
```

You cannot enter the `wccp-cache-engine enable` command if you have already added a WCCP service group. When you enter this command an interface named w.<vdom_name> is added to the FortiGate configuration (for example w.root). All traffic redirected from a WCCP router is considered to be received at this interface of the FortiGate unit operating as a WCCP client. A default route to this interface with lowest priority is added.

Example WCCP server and client configuration for caching HTTPS sessions

Enter the following command to add a service group to a WCCP server that caches HTTPS content on port 443 and protocol 6. The IP address of the server is 10.31.101.100 and the WCCP clients are on the 10.31.101.0 subnet. The service ID of this service group is 80.

```
config system wccp
   edit 80
      set router-id 10.31.101.100
      set server-list 10.31.101.0 255.255.255.0
      set ports 443

      set protocol 6
   end
```

Enter the following commands to configure a FortiGate unit to operate as a WCCP client and add a service group that configures client to cache HTTPS sessions on port 443 and protocol 6. The IP address of the server is 10.31.101.100 and IP address of this WCCP clients is 10.31.101.1 subnet. The service ID of this service group must be 80 to match the service ID added to the server.

```
config system settings
   set wccp-cache-engine enable
end

config system wccp
   edit 80
      set cache-id 10.31.101.1
      set router-list 10.31.101.100
      set ports 443
      set protocol 6
   end
```

Example WCCP server and client configuration for caching HTTP and HTTPS sessions

You could do this by configuring two WCCP service groups as described in the previous examples. Or you could use the following commands to configure one service group for both types of traffic. The example also caches HTTP sessions on port 8080.

Enter the following command to add a service group to a WCCP server that caches HTTP sessions on ports 80 and 8080 and HTTPS sessions on port 443. Both of these protocols use protocol number 6. The IP address of the server is 10.31.101.100 and the WCCP clients are on the 10.31.101.0 subnet. The service ID of this service group is 90.

```
config system wccp
   edit 90
      set router-id 10.31.101.100
      set server-list 10.31.101.0 255.255.255.0
      set ports 443 80 8080
      set protocol 6
   end
```

Enter the following commands to configure a FortiGate unit to operate as a WCCP client and add a service group that configures client to cache HTTP sessions on port 80 and 8080 and HTTPS sessions on port 443. The IP address of the server is 10.31.101.100 and IP address of this WCCP clients is 10.31.101.1 subnet. The service ID of this service group must be 90 to match the service ID added to the server.

```
config system settings
   set wccp-cache-engine enable
end
config system wccp
   edit 90
      set cache-id 10.31.101.1
      set router-list 10.31.101.100
      set ports 443 80 8080
      set protocol 6
   end
```

Other WCCP service group options

In addition to using WCCP service groups to define the types of traffic to be cached by WCCP the following options are available for servers and clients.

Server configuration options

The server configuration must include the `router-id`, which is the WCCP server IP address. This is the IP address of the interface that the server uses to communicate with WCCP clients.

The `group-address` is used for multicast WCCP configurations to specify the multicast addresses of the clients.

The `server-list` defines the IP addresses of the WCCP clients that the server can connect to. Often the server list can be the address of the subnet that contains the WCCP clients.

The `authentication` option enables or disables authentication for the WCCP service group. Authentication must be enabled on all servers and clients in a service group and members of the group must have the same `password`.

The `forward-method` option specifies the protocol used for communication between the server and clients. The default forwarding method is GRE encapsulation. If required by your network you can also select to use unencapsulated layer-2 packets instead of GRE or select any to allow both. The `return-method` allows you to specify the communication method from the client to the server. Both GRE and layer-2 are supported.

The `assignment-method` determines how the server load balances sessions to the clients if there are multiple clients. Load balancing can be done using hashing or masking.

Client configuration options

The client configuration includes the `cache-id` which is the IP address of the FortiGate interface of the client that communicates with WCCP server. The `router-list` option is the list of IP addresses of the WCCP servers in the WCCP service group.

The `ports` option lists the port numbers of the sessions to be cached by the client and the `protocol` sets the protocol number of the sessions to be cached. For TCP sessions the protocol is 6.

The `service-type` option can be auto, dynamic or standard. Usually you would not change this setting.

The client configuration also includes options to influence load balancing including the `primary-hash`, `priority`, `assignment-weight` and `assignment-bucket-format`.

WCCP configuration overview

To configure WCCP you must create a service group that includes WCCP servers and clients. WCCP servers intercept sessions to be cached (for example, sessions from users browsing the web from a private network). To intercept sessions to be cached the WCCP server must include a security policy that accepts sessions to be cached and WCCP must be enabled in this security policy.

The server must have an interface configured for WCCP communication with WCCP clients. That interface sends and receives encapsulated GRE traffic to and from WCCP clients. The server must also include a WCCP service group that includes a service ID and the addresses of the WCCP clients as well as other WCCP configuration options.

To use a FortiGate unit as a WCCP client, the FortiGate unit must be set to be a WCCP client (or cache engine). You must also configure an interface on the client for WCCP communication. The client sends and receives encapsulated GRE traffic to and from the WCCP server using this interface.

The client must also include a WCCP service group with a service ID that matches a service ID on the server. The client service group also includes the IP address of the servers in the service group and specifies the port numbers and protocol number of the sessions that will be cached on the client.

When the client receives sessions from the server on its WCCP interface, it either returns cached content over the WCCP interface or connects to the destination web servers using the appropriate interface depending on the client routing configuration. Content received from web servers is then cached by the client and returned to the WCCP server over the WCCP link. The server then returns the received content to the initial requesting user web browser.

Finally you may also need to configure routing on the server and client FortiGate units and additional security policies may have to be added to the server to accept sessions not cached by WCCP.

Example caching HTTP sessions on port 80 using WCCP

In this example configuration (shown below), a FortiGate unit with host name WCCP_srv is operating as an Internet firewall for a private network is also configured as a WCCP server. The port1 interface of WCCP_srv is connected to the Internet and the port2 interface is connected to the internal network.

All HTTP traffic on port 80 that is received at the port2 interface of WCCP_srv is accepted by a port2 to port1 security policy with WCCP enabled. All other traffic received at the port2 interface is allowed to connect to the Internet by adding a general port2 to port1 security policy below the HTTP on port 80 security policy.

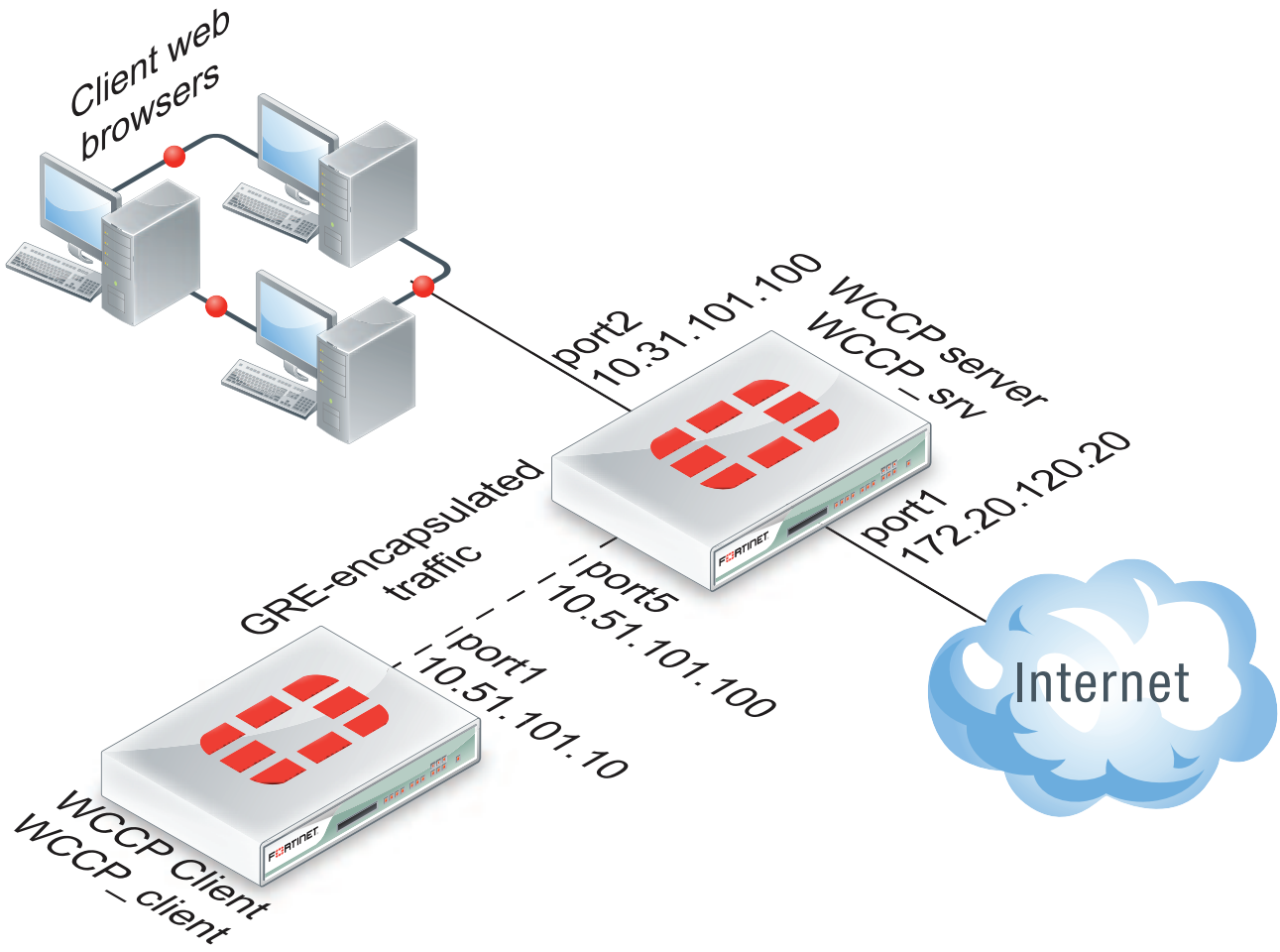
A WCCP service group is added to WCCP_srv with a service ID of 0 for caching HTTP traffic on port 80. The port5 interface of WCCP_srv is configured for WCCP communication.

A second FortiGate unit with host name WCCP_client is operating as a WCCP client. The port1 interface of WCCP_client is connected to port5 of WCCP_srv and is configured for WCCP communication.

WCCP_client is configured to cache HTTP traffic because it also has a WCCP service group with a service ID of 0.

WCCP_client connects to the Internet through WCCP_srv. To allow this, a port5 to port1 security policy is added to WCCP_srv.

FortiGate WCCP server and client configuration



Configuring the WCCP server (WCCP_srv)

Use the following steps to configure WCCP_srv as the WCCP server for the example network. The example steps only describe the WCCP-related configuration.

To configure WCCP_srv as a WCCP server

1. Add a port2 to port1 security policy that accepts HTTP traffic on port 80 and is configured for WCCP:

```
config firewall policy
   edit 0
      set srtintf port2
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP
      set wccp enable
      set nat enable
   end
```

2. Add another port2 to port1 security policy to allow all other traffic to connect to the Internet.

```
config firewall policy
   edit 0
      set srtintf port2
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set nat enable
   end
```

3. Move this policy below the WCCP policy in the port2 to port1 policy list.
4. Enable WCCP on the port5 interface.

```
config system interface
   edit port5
      set wccp enable
   end
```

5. Add a WCCP service group with service ID 0.

```
config system wccp
   edit 0
      set router-id 10.51.101.100
      set server-list 10.51.101.0 255.255.255.0
   end
```

6. Add a firewall address and security policy to allow the WCCP_client to connect to the internet.

```
config firewall address
   edit WCCP_client_addr
      set subnet 10.51.101.10
end
config firewall policy
   edit 0
      set srtintf port5
      set dstintf port1
      set srcaddr WCCP_client_addr
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set nat enable
   end
```

Configuring the WCCP client (WCCP_client)

Use the following steps to configure WCCP_client as the WCCP client for the example network. The example steps only describe the WCCP-related configuration.

To configure WCCP_client as a WCCP client

1. Configure WCCP_client to operate as a WCCP client.

```
config system settings
   set wccp-cache-engine enable
```

```
end
```

You cannot enter the `wccp-cache-engine enable` command if you have already added a WCCP service group. When you enter this command an interface named w.<vdom_name> is added to the FortiGate configuration (for example w.root). All traffic redirected from a WCCP router is considered to be received at this interface of the FortiGate unit operating as a WCCP client. A default route to this interface with lowest priority is added.

2. Enable WCCP on the port1 interface.

```
config system interface
   edit port1
      set wccp enable
end
```

3. Add a WCCP service group with service ID 0.

```
config system wccp
   edit 0
      set cache-id 10.51.101.10
      set router-list 10.51.101.100
end
```

Example caching HTTP sessions on port 80 and HTTPS sessions on port 443 using WCCP

This example configuration is the same as thatdescribed in Example caching HTTP sessions on port 80 using WCCP on page 2939 except that WCCP now also cached HTTPS traffic on port 443. To cache HTTP and HTTPS traffic the WCCP service group must have a service ID in the range 51 to 255 and you must specify port 80 and 443 and protocol 6 in the service group configuration of the WCCP client.

Also the security policy on the WCCP_srv that accepts sessions from the internal network to be cached must accept HTTP and HTTPS sessions.

Configuring the WCCP server (WCCP_srv)

Use the following steps to configure WCCP_srv as the WCCP server for the example network. The example steps only describe the WCCP-related configuration.

To configure WCCP_srv as a WCCP server

1. Add a port2 to port1 security policy that accepts HTTP traffic on port 80 and HTTPS traffic on port 443 and is configured for WCCP:

```
config firewall policy
   edit 0
      set srtintf port2
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP HTTPS
      set wccp enable
      set nat enable
```

```
end
```

2. Add another port2 to port1 security policy to allow all other traffic to connect to the Internet.

```
config firewall policy
   edit 0
      set srtintf port2
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ANY

      set nat enable
   end
```

3. Move this policy below the WCCP policy in the port2 to port1 policy list.
4. Enable WCCP on the port5 interface.

```
config system interface
   edit port5
      set wccp enable
   end
```

5. Add a WCCP service group with service ID 90 (can be any number between 51 and 255).

```
config system wccp
   edit 90
      set router-id 10.51.101.100
      set server-list 10.51.101.0 255.255.255.0
   end
```

6. Add a firewall address and security policy to allow the WCCP_client to connect to the internet.

```
config firewall address
   edit WCCP_client_addr
      set subnet 10.51.101.10
   end
config firewall policy
   edit 0
      set srtintf port5
      set dstintf port1
      set srcaddr WCCP_client_addr
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set nat enable
   end
```

Configuring the WCCP client (WCCP_client)

Use the following steps to configure WCCP_client as the WCCP client for the example network. The example steps only describe the WCCP-related configuration.

To configure WCCP_client as a WCCP client

1. Configure WCCP_client to operate as a WCCP client.

```
config system settings
   set wccp-cache-engine enable
end
```

You cannot enter the `wccp-cache-engine enable` command if you have already added a WCCP service group. When you enter this command an interface named w.<vdom_name> is added to the FortiGate configuration (for example w.root). All traffic redirected from a WCCP router is considered to be received at this interface of the FortiGate unit operating as a WCCP client. A default route to this interface with lowest priority is added.

2. Enable WCCP on the port1 interface.

```
config system interface
   edit port1
      set wccp enable
   end
```

3. Add a WCCP service group with service ID 90. This service group also specifies to cache sessions on ports 80 and 443 (for HTTP and HTTPS) and protocol number 6.

```
config system wccp
   edit 90
      set cache-id 10.51.101.10
      set router-list 10.51.101.100
      ports 80 443
      set protocol 6
   end
```

WCCP packet flow

The following packet flow sequence assumes you have configured a FortiGate unit to be a WCCP server and one or more FortiGate units to be WCCP clients.

1. A user's web browser sends a request for web content.
2. The FortiGate unit configured as a WCCP server includes a security policy that intercepts the request and forwards it to a WCCP client.

   The security policy can apply UTM features to traffic accepted by the policy.
3. The WCCP client receives the WCCP session.
4. The client either returns requested content to the WCCP server if it is already cached, or connects to the destination web server, receives and caches the content and then returns it to the WCCP server.
5. The WCCP server returns the requested content to the user's web browser.
6. The WCCP router returns the request to the client web browser.

   The client we browser is not aware that all this is taking place and does not have to be configured to use a web proxy.

Configuring the forward and return methods and adding authentication

The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP router to the WCCP cache engine. There are two different forwarding methods:

- GRE forwarding (the default) encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP router and a destination IP address of the target WCCP cache engine. The results is a tunnel that allows the WCCP router to be multiple hops away from the WCCP cache server.
- L2 forwarding rewrites the destination MAC address of the intercepted packet to match the MAC address of the target WCCP cache engine. L2 forwarding requires that the WCCP router is Layer 2 adjacent to the WCCP client.

You can use the following command on a FortiGate unit configured as a WCCP router to change the forward and return methods to L2:

```
config system wccp
   edit 1
      set forward-method L2
      set return-method L2
end
```

You can also set the forward and return methods to any in order to match the cache server configuration.

By default the WCCP communication between the router and cache servers is unencrypted. If you are concerned about attackers sniffing the information in the WCCP stream you can use the following command to enable hash-based authentication of the WCCP traffic. You must enable authentication on the router and the cache engines and all must have the same password.

```
config system wccp
   edit 1
      set authentication enable
      set password <password>
end
```

WCCP Messages

When the WCCP service is active on a web cache server it periodically sends a WCCP HERE I AM broadcast or unicast message to the FortiGate unit operating as a WCCP router. This message contains the following information:

- Web cache identity (the IP address of the web cache server).
- Service info (the service group to join).

If the information received in the previous message matches what is expected, the FortiGate unit replies with a WCCP I SEE YOU message that contains the following details:

- Router identity (the FortiGate unit's IP address.
- Sent to IP (the web cache IP addresses to which the packets are addressed)

When both ends receive these two messages the connection is established, the service group is formed and the designated web cache is elected.

Troubleshooting WCCP

Two types of debug commands are available for debugging or troubleshooting a WCCP connection between a FortiGate unit operating as a WCCP router and its WCCP cache engines.

Real time debugging

The following commands can capture live WCCP messages:

```
diag debug en
diag debug application wccpd <debug level>
```

Application debugging

The following commands display information about WCCP operations:

```
get test wccpd <integer>
diag test application wccpd <integer>
```

Where `<integer>` is a value between 1 and 6:

1. Display WCCP stats
2. Display WCCP config
3. Display WCCP cache servers
4. Display WCCP services
5. Display WCCP assignment
6. Display WCCP cache status

Enter the following command to view debugging output:

```
diag test application wccpd 3
```

Sample output from a successful WCCP connection:

```
service-0 in vdom-root: num=1, usable=1
cache server ID:
len=44, addr=172.16.78.8, weight=4135, status=0
rcv_id=6547, usable=1, fm=1, nq=0, dev=3(k3),
to=192.168.11.55
ch_no=0, num_router=1:
192.168.11.55
```

Sample output from the same command from an unsuccessful WCCP connection (because of a service group password mismatch):

```
service-0 in vdom-root: num=0, usable=0
diag debug application wccpd -1
Sample output:
wccp_on_recv()-98: vdom-root recv: num=160, dev=3(3),
172.16.78.8->192.168.11.55
wccp2_receive_pkt()-1124: len=160, type=10, ver=0200,
length=152
wccp2_receive_pkt()-1150: found component:t=0, len=20
wccp2_receive_pkt()-1150: found component:t=1, len=24
wccp2_receive_pkt()-1150: found component:t=3, len=44
wccp2_receive_pkt()-1150: found component:t=5, len=20
wccp2_receive_pkt()-1150: found component:t=8, len=24
wccp2_check_security_info()-326: MD5 check failed
```

Diagnose commands

The following get and diagnose commands are available for troubleshooting WAN optimization, web cache, explicit proxy and WCCP.

get test {wad | wccpd} <test_level>

Display usage information about WAN optimization, explicit proxy, web cache, and WCCP applications. Use `<test_level>` to display different information.

```
get test wad <test_level>
get test wccpd <test_level>
```

Variable	Description
wad	Display information about WAN optimization, web caching, the explicit web proxy, and the explicit FTP proxy.
wccpd	Display information about the WCCP application.

Examples

Enter the following command to display WAN optimization tunnel protocol statistics. The http tunnel and tcp tunnel parts of the command output below shows that WAN optimization has been processing HTTP and TCP packets.

```
get test wad 1
WAD manager process status: pid=113 n_workers=1 ndebug_workers=0
```

Enter the following command to display all test options:

```
get test wad

WAD process 82 test usage:
   1: display process status
   2: display total memory usage.
   99: restart all WAD processes
   1000: List all WAD processes.
   1001: dispaly debug level name and values
   1002: dispaly status of WANOpt storages
   1068: Enable debug for all WAD workers.
   1069: Disable debug for all WAD workers.
   2yxx: Set No. xx process of type y as diagnosis process.
   3: display all fix-sized advanced memory stats
   4: display all fix-sized advanced memory stats in details
   500000..599999: cmem bucket stats (599999 for usage)
   800..899: mem_diag commands (800 for help & usage)
   800000..899999: mem_diag commands with 1 arg (800 for help & usage)
   80000000..89999999: mem_diag commands with 2 args (800 for help & usage)
   60: show debug stats.
   61: discard all wad debug info that is currently pending
   62xxx: set xxxM maximum ouput buffer size for WAD debug. 0, set back to default.
   68: Enable process debug
```

```
    69: Disable process debug
    98: gracefully stopping WAD process
    9xx: Set xx workers(0: default based on user configuration.)
```

diagnose wad

Display diagnostic information about the WAN optimization daemon (wad).

```
diagnose wad console-log {disable | enable)
diagnose wad debug-url {disable | enable)
diagnose wad filter {clear | dport | dst | list | negate | protocol | sport | src | vd}
diagnose wad history {clear | list}
diagnose wad session {clear | list}
diagnose wad stats {cache | cifs | clear | crypto | ftp | http | list | mapi | mem |
    scan | scripts | summary | tcp | tunnel}
diagnose wad user {clear | list}
diagnose wad tunnel {clear | list}1
diagnose wad webcache {clear | list} {10min | hour | day | 30days}
```

Variable	Description
`console-log`	Enable or disable displaying WAN optimization log messages on the CLI console.
`filter`	Set a filter for listing WAN optimization daemon sessions or tunnels. `clear` reset or clear the current log filter settings. `dport` enter the destination port range to filter by. `dst` enter the destination address range to filter by. `list` display the current log filter settings
`history`	Display statistics for one or more WAN optimization protocols for a specified period of time (the last 10 minutes, hour, day or 30 days).
`session`	Display diagnostics for WAN optimization sessions or clear active sessions.
`stats`	Display statistics for various parts of WAN optimization such as cache statistics, CIFS statistics, MAPI statistics, HTTP statistics, tunnel statistics etc. You can also clear WAN optimization statistics and display a summary.
`tunnel`	Display diagnostic information for one or all active WAN optimization tunnels. Clear all active tunnels. Clear all active tunnels.
`webcache`	Display web cache activity for the specified time period.

Example diagnose wad tunnel list

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output shows 10 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to off).

```
diagnose wad tunnel list

Tunnel: id=100 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=100 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=348 bytes_out=384

Tunnel: id=99 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=99 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=348 bytes_out=384

Tunnel: id=98 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=98 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=348 bytes_out=384

Tunnel: id=39 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=39 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1068 bytes_out=1104

Tunnel: id=7 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=7 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=8 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=8 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=5 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=5 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=4 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=4 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=1 type=manual
   vd=0 shared=no uses=0 state=3
   peer name=Web_servers id=1 ip=172.20.120.141
   SSL-secured-tunnel=no auth-grp=
   bytes_in=1228 bytes_out=1264

Tunnel: id=2 type=manual
```

```
    vd=0 shared=no uses=0 state=3
    peer name=Web_servers id=2 ip=172.20.120.141
    SSL-secured-tunnel=no auth-grp=
    bytes_in=1228 bytes_out=1264

Tunnels total=10 manual=10 auto=0
```

Example diagnose wad webcache list

This following command displays the web caching stats for the last 10 minutes of activity. The information displayed is divided into 20 slots and each slot contains stats for 30 seconds:

20 * 30 seconds = 600 seconds = 10 minutes

```
diagnose wad webcache list 10min
web cache history vd=0 period=last 10min
```

The first 20 slots are for HTTP requests in the last 10 minutes. Each slot of stats has four numbers, which is the total number of HTTP requests, the number of cacheable HTTP requests, the number of HTTP requests that are processed by the web cache (hits), and the number of HTTP requests that are processed without checking the web cache (bypass). There are many reasons that a HTTP request may bypass web cache.

```
total        cacheable     hits          bypass
------------ ------------- ------------ -------------
36           10            3            1
128          92            1            10
168          97            2            3
79           56            0            3
106          64            5            3
180          118           6            11
88           53            7            3
80           43            4            4
107          44            9            2
84           12            0            2
228          139           52           10
32           2             0            5
191          88            13           7
135          25            40           3
48           10            0            8
193          13            7            7
67           31            1            2
109          35            24           6
117          36            10           5
22           0             0            4
```

The following slots are for video requests in the last 10 minutes. Each slot has two numbers for each 30 seconds: total number of video requests, and the number of video requests that are processing using cached data.

```
video total  video hit
------------ -------------
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
0            0
```

The following 20 slots are for traffic details in last 10 minutes. Each slot has four numbers for 30 seconds each.

```
--- LAN ---                 --- WAN ---
bytes_in     bytes_out      bytes_in     bytes_out
------------ -------------- ------------ -------------
34360        150261         141086       32347
105408       861863         858501       100670
128359       1365919        1411849      127341
60103        602813         818075       59967
105867       1213192        1463736      97489
154961       1434784        1344911      158667
73967        370275         369847       70626
129327       602834         592399       123676
115719       663446         799445       111262
58151        724993         631721       59989
175681       2092925        1092556      166212
37805        33042          41528        37779
183686       1255118        1114646      172371
106125       904178         807152       81520
66147        473983         543507       66782
170451       1289530        1201639      165540
69196        544559         865370       68446
134142       579605         821430       132113
96895        668037         730633       89872
59576        248734         164002       59448
```

diagnose wacs

Display diagnostic information for the web cache database daemon (wacs).

```
diagnose wacs clear
diagnose wacs recents
diagnose wacs restart
diagnose wacs stats
```

Variable	Description
clear	Remove all entries from the web cache database.
recents	Display recent web cache database activity.
restart	Restart the web cache daemon and reset statistics.
stats	Display web cache statistics.

diagnose wadbd

Display diagnostic information for the WAN optimization database daemon (waddb).

```
diagnose wadbd {check | clear | recents | restart | stats}
```

Variable	Description
check	Check WAN optimization database integrity.
clear	Remove all entries from the WAN optimization database.
recents	Display recent WAN optimization database activity.
restart	Restart the WAN optimization daemon and reset statistics.
stats	Display WAN optimization statistics.

diagnose debug application {wad | wccpd} [<debug_level>]

View or set the debug level for displaying WAN optimization and web cache-related daemon debug messages. Include a <debug_level> to change the debug level. Leave the <debug_level> out to display the current debug level. Default debug level is 0.

```
diagnose debug application wad [<debug_level>]
diagnose debug application wccpd [<debug_level>]
```

Variable	Description
wad	Set the debug level for the WAN optimization daemon.
wccpd	Set the debug level for the WCCP daemon.

diagnose test application wad 2200

The debug level 2200 switches the debug to explicit proxy mode. You have to enter this debug level first. After that you have to type the command again with a different debug level to check the different explicit proxy statistics. To list what each debug level shows, follow these steps in any FortiGate device:

1. Enable explicit proxy globally and in one interface, to start the wad process. If the wad process is *not* running, you *cannot* list the options.
2. Once the wad process starts, type:

```
diagnose test application wad 2200
diagnose test application wad  ///// Do not type any debug level value to list all the options.
```

This is the output you will get:

```
# diagnose test application wad 2200
Set diagnosis process: type=wanopt index=0 pid=114
# diagnose test application wad
WAD process 114 test usage:
1: display process status
2: display total memory usage
99: restart all WAD processes
1000: List all WAD processes
1001: dispaly debug level name and values
1002: dispaly status of WANOpt storages
1068: Enable debug for all WAD workers
1069: Disable debug for all WAD workers
2yxx: Set No. xx process of type y as diagnosis process
3: display all fix-sized advanced memory stats
4: display all fix-sized advanced memory stats in details
500000..599999: cmem bucket stats (599999 for usage)
800..899: mem_diag commands (800 for help & usage)
800000..899999: mem_diag commands with 1 arg (800 for help & usage)
80000000..89999999: mem_diag commands with 2 args (800 for help & usage)
60: show debug stats
61: discard all wad debug info that is currently pending
62xxx: set xxxM maximum ouput buffer size for WAD debug (0: set back to default)
68: Enable process debug
69: Disable process debug
98: gracefully stopping WAD process
20: display all listeners
21: display TCP port info
22: display SSL stats
23: flush SSL stats
24: display SSL mem stats
70: display av memory usage
71xxxx: set xxxxMiB maximum AV memory (0: set back to default)
72: toggle av memory protection
73: toggle AV conserve mode (for debug purpose)
90: set to test disk failure
91: unset to test disk failure
92: trigger a disk failure event
100: display explicit proxy settings
101: display firewall policies
102: display security profile mapping for regular firewall policy
103: display Web proxy forwarding server and group
104: display DNS stats
105: display proxy redirection scan stats
106: list all used fqdns
107: list all firewall address
110: display current web proxy users
111: flush current web proxy users
112: display current web proxy user summary
```

```
113: display WAD fsso state
114: display HTTP digest stats
115: display URL patterns list of cache exemption or forward server
116: toggle dumping URL when daemon crashes
120: display Web Cache stats
121: flush Web Cache stats
122: flush idle Web cache objects
123: display web cache cache sessions
130: display ftpproxy stats
131: clear ftpproxy stats
132: list all current ftpproxy sessions
133: display all catched webfilter profiles
200: display WANopt profiles
201: display all peers
202: display video cache rules (patterns)
203: display all ssl servers
210: toggle disk-based byte-cache
211: toggle memory-based byte-cache
212: toggle cifs read-ahead
221: display tunnel protocol stats
222: flush tunnel protocol stats
223: display http protocol stats
224: flush http protocol stats
225: display cifs protocol stats
226: flush cifs protocol stats
227: display ftp protocol stats
228: flush ftp protocol stats
229: display mapi protocol stats
230: flush mapi protocol stats
231: display tcp protocol stats
232: flush tcp protocol stats
233: display all protocols stats
234: flush all protocols stats
240: display WAD tunnel stats
241: display tunnel compressor state
242: flush tunnel compressor stats
243: display Byte Cache DB state
244: flush Byte Cache DB stats
245: display Web Cache DB state
246: flush Web Cache DB stats
247: display cache state
248: flush cache stats
249: display memory cache state
250: flush memory cache stats
261yxxx: set xxx concurrent Web Cache session for object storage y
262yxxx: set xxxK(32K, 64K,...) unconfirmed write/read size per Web Cache object for
    object storage y
263yxxxx: set xxxxK maximum ouput buffer size for object storage y
264yxx: set lookup lowmark (only if more to define busy status) to be xx for object
    storage y
265yxxx: set xxxK maximum ouput buffer size for byte storage y
266yxxx: set number of buffered add requests to be xxx for byte storage y
267yxxxx: set number of buffered query requests to be xxxx for byte storage y
268yxxxxx: set number of concurrent query requests to be xxxxx for byte storage y
```

Appendix A - Open Ports Diagrams

Open Ports Diagrams

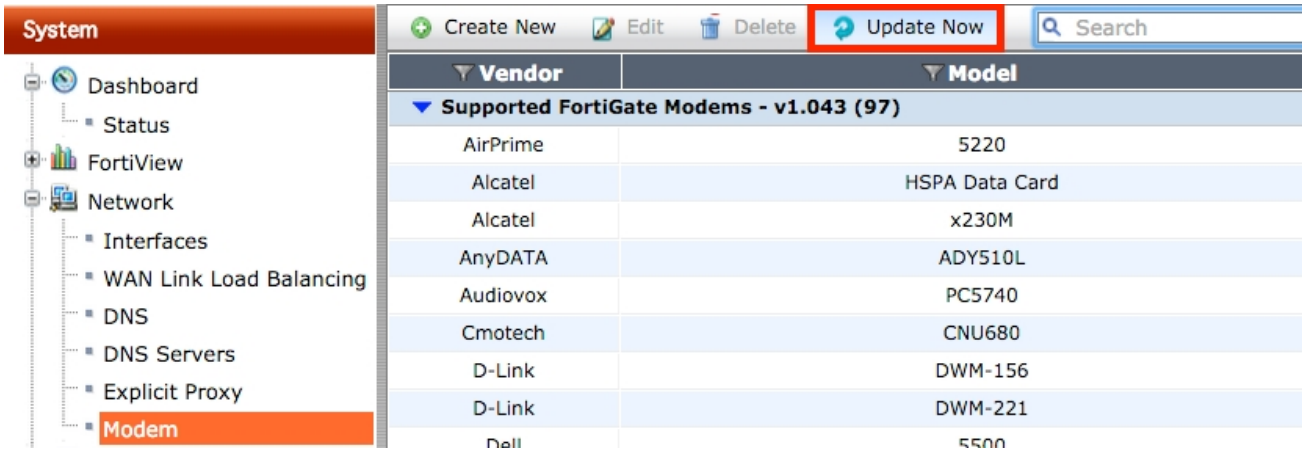
Appendix B - FortiGate Modem Compatibility Matrix

FortiGate Modem Compatibility Matrix

The list of supported modems below depends on the modem database version and not on the version of FortiOS. You can also find the list in the FortiOS web-based interface, however this document may include more recent updates before they appear in the web-based interface list.

To find the modem list (FortiOS 5.2) - web-based manager:

1. Go to **System > Network > Modem** and under **External Modem** select **[Configure Modem]**.
2. Click the **Update Now** button to get the latest version of the **Supported FortiGate Modems** list.



3. Verify that the version number has updated, and select a list to open it.

The modems are listed in alphabetical order.

Vendor	Model	Network
AirPrime	5220	3G
Alcatel	HSPA Data Card	3G
Alcatel	x230M	3G
AnyDATA	ADY510L	3G
Audiovox	PC5740	3G
Cmotech	CNU680	3G
D-Link	DWM-156	3G

Vendor	Model	Network
D-Link	DWM-221	3G
Dell	5500	3G
Emobile	D11LC	3G
Emobile	ST Mobile	3G
Franklin	S600C	3G
Huawei	E126	3G
Huawei	E169	3G
Huawei	E1692/E303H	3G
Huawei	E173	3G
Huawei	E303	4G
Huawei	E180/E220/E3735	3G
Huawei	E220/E3735	3G
Huawei	E353	3G
Huawei	E372	3G
Huawei	E392	3G
Huawei	E392/E397/E398	3G
Huawei	E392/E397/E353/E3276	3G
Huawei	E398	3G
Huawei	E586	4G
Huawei	E600/E169	3G
Huawei	E3276	4G
Huawei	K3715	3G
Huawei	K3765	3G
Huawei	K3770	3G
Huawei	K3773	3G

Vendor	Model	Network
Huawei	K3773/E3131	3G
Huawei	K3806	3G
Huawei	K4201	4G
Huawei	K4505	3G
Huawei	K4511	3G
Huawei	K5150	4G
Kyocera	KPC650/Passport	3G
LG	L-02C	3G
LG	L-03D	3G
Maxon	USB3-8521	3G
MobiData	MBD-200HU	3G
NCXX Inc.	NCXX US302NC	3G
Novatel	ExpressCard34 Qualcomm 3G CDMA	3G
Novatel	MC679	4G
Novatel	MC990D	3G
Novatel	Merlin EX720	3G
Novatel	Merlin S620	3G
Novatel	Merlin S720	3G
Novatel	Merlin X950D	3G
Novatel	Merlin XU870	3G
Novatel	Ovation MC950D	3G
Novatel	Ovation MC998D	3G
Novatel	Ovation U720	3G
Novatel	Ovation U727	3G
Novatel	U760	3G

Vendor	Model	Network
Novatel	U998	3G
Option	GI1505	3G
Option	GI332	3G
Option	iCON 225 HSDPA	3G
Option	N.V. Globetrotter Fusion Quad Lite	3G
Option	N.V. Globetrotter HSDPA Modem	3G
Pantech	PX-500	3G
Pantech	UM190	3G
Pantech	UML290	3G
Quanta	MU-Q101	3G
Sierra	250U	3G
Sierra	597	3G
Sierra	598U	3G
Sierra	AC312U/AC503/USB306/USB308	3G
Sierra	AC313U	4G
Sierra	AC320U	3G
Sierra	AC330U	3G
Sierra	AC340U	3G
Sierra	AC501/880E	3G
Sierra	AirCard 580	3G
Sierra	AirCard 595	3G
Sierra	AirCard 595U	3G
Sierra	AirCard 875	3G
Sierra	C885	3G
Sierra	EM5625	3G

Vendor	Model	Network
Sierra	MC5720	3G
Sierra	MC5728	3G
Sierra	UC881	3G
Sprint	U300	3G
Teracom	LW273	3G
ZTE	AC2736	3G
ZTE	MF180	3G
ZTE	MF190	3G
ZTE	MF190U	3G
ZTE	MF626	3G
ZTE	MF637	3G
ZTE	MF667	49
ZTE	MF668	3G
ZTE	MF680	3G
ZTE	MF683	3G
ZTE	MF691	3G
ZTE	MF820	3G
ZTE	MF821	3G
ZTE	MY39	3G

This table is a work-in-progress. Please contact techdoc@fortinet.com if you have suggestions for improvements.

CHANGE LOG

March 17, 2016	Updated release for Supported FortiGate Modem list v.1.043. Updated 4G supported modems list to reflect new changes (Internal tracking no. 0248344). The new supported 4G modems now include: Sierra AirCard 313U, Huawei K5150, Huawei K4201, Huawei E303, Huawei E3276, Huawei E586 and the ZTE MF667. This update also includes removal of certain models from the 4G category based on compatibility issues.

CHANGE LOG

Nov 2, 2015	Updated to include 3G or 4G capabilities for each modem.
May 21, 2015	Updated release for Supported FortiGate Modems list v1.031.
October 29, 2014	Updated to include FortiGate supported modems.
September 5, 2014	Initial release.

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Appendix C - FortiExtender Modem Compatibility Matrix

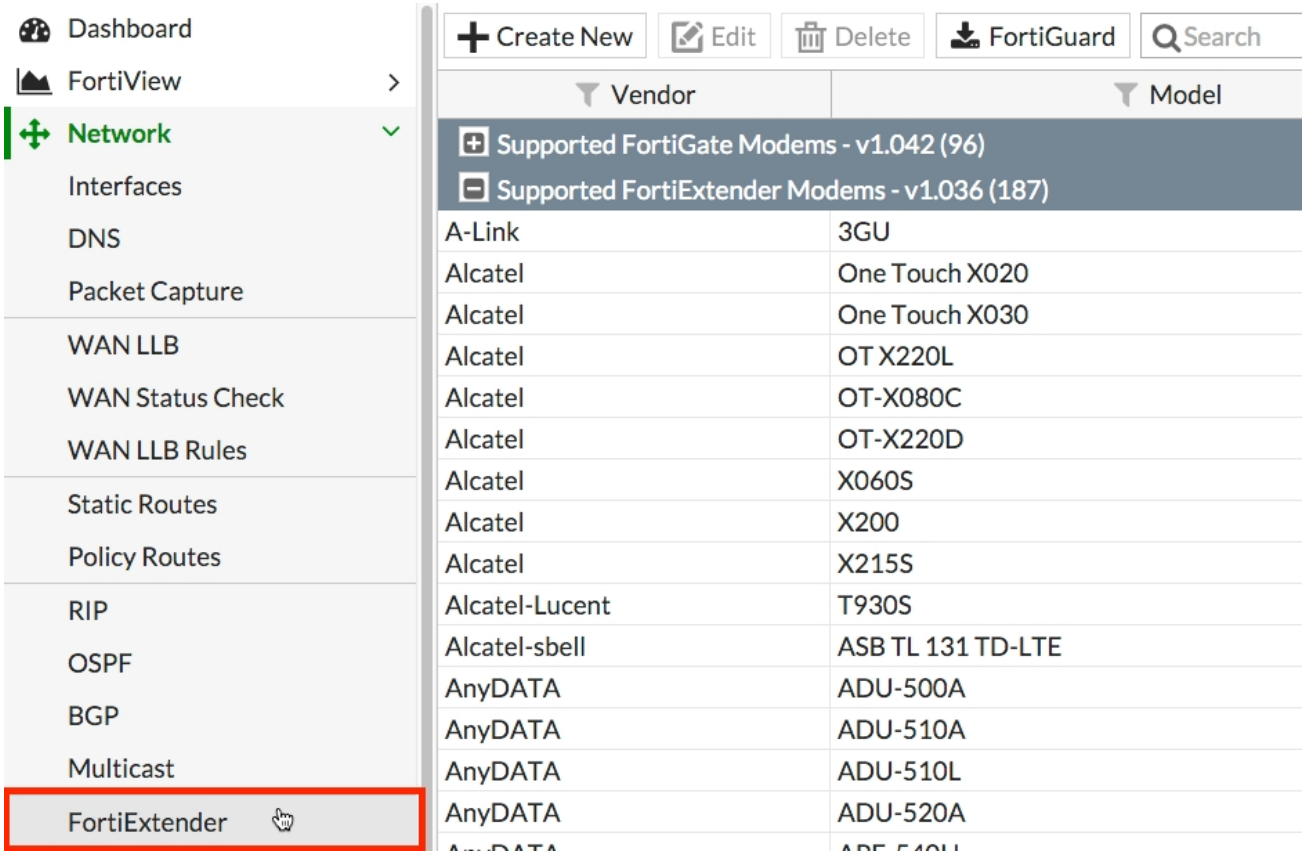
FortiExtender Modem Compatibility Matrix

The following table lists the USB modems currently supported by FortiExtender.The list of supported modems below depends on the modem database version and not on the version of FortiOS. They are listed in alphabetical order. You can also find the list in the FortiOS web-based interface, however this document may include more recent updates before they appear in the web-based interface list.

Note: FEX-100A has an internal modem, and therefore doesn't support external USB modems.

To find the FortiExtender Modem list (FortiOS 5.2) - web-based manager:

1. Go to **System > Feature Select** and enable **FortiExtender**.
2. Go to **Network > FortiExtender** and select **Configure Settings.**
3. Under **Modem Settings**, select **[Supported Modems]**.
4. Click the **Update Now** button to get the latest version of the **Supported FortiGate Modems** list.



5. Verify that the version number has updated, and select **Supported FortiExtender Modems**.

Vendor	Model
A-Link	3GU
Alcatel	One Touch X020
Alcatel	One Touch X030
Alcatel	OT X220L
Alcatel	OT-X080C
Alcatel	OT-X220D
Alcatel	X060S
Alcatel	X200
Alcatel	X215S
Alcatel-Lucent	T930S
Alcatel-sbell	ASB TL 131 TD-LTE
AnyDATA	ADU-500A
AnyDATA	ADU-510A
AnyDATA	ADU-510L
AnyDATA	ADU-520A
AnyDATA	APE-540H
Axesstel	MU130
BandLuxe	C120
BandRich	BandLuxe C170
BandRich	BandLuxe C270
BandRich	BandLuxe C339
Beceem	BCSM250
C-motech	CDU-680
C-motech	CDU-685a

Vendor	Model
C-motech	CGU-628
C-motech	CHU-628S
C-motech	CHU-629S
C-motech	D-50
Celot	CT-680
Celot	K-300
Changhong	CH690
China TeleCom	CBP7.0
D-Link	DWM-156
D-Link	DWM-162-US
D-Link	DWR-510
Digicom	8E4455
EpiValley	SEC-7089
Exiss Mobile	E-190 series
Franklin Wireless	CGU-628A
Franklin Wireless	U210
Franklin Wireless	U600
GW	D301
Haier	CE 100
Haier	CE682 (EVDO)
Huawei	E1550
Huawei	E1612
Huawei	E169
Huawei	E1690

Vendor	Model
Huawei	E1692
Huawei	E171
Huawei	E173
Huawei	E1750
Huawei	E1762
Huawei	E177
Huawei	E180
Huawei	E1820
Huawei	E270+
Huawei	E3251
Huawei	E3276s-151
Huawei	E352
Huawei	E353
Huawei	E355s-1
Huawei	E535
Huawei	E587
Huawei	E630
Huawei	EC156
Huawei	EC168C
Huawei	ET302
Huawei	ET8282
Huawei	GP02
Huawei	K3765
Huawei	K3770

Vendor	Model
Huawei	K3771
Huawei	K3772
Huawei	K4305
Huawei	K4505
Huawei	K4605
Huawei	R201
Huawei	U7510
Huawei	U7517
Huawei	U8110
Huawei	U8220
Huawei	U8300
I-O Data	WMX2-U Wimax
JOA Telecom	LM-700r
KDDI (Huawei)	HWD12 LTE
Kyocera	W06K
LG	AD600
LG	HDM-2100
LG	L-02C LTE
LG	L-03D
LG	L-05A
LG	L-07A
LG	L-08C
LG	LDU-1900D
LG	LUU-2100TI (aka AT&T USBConnect Turbo)

Vendor	Model
LG	SD711
Mediatek	MT6229
MediaTek	MT6276M
MediaTek	Wimax USB Card
Micromax	MMX 300c
MobiData	MBD-200HU
Netgear	WNDA3200
Netgear (Sierra Wireless)	AC313U
Netgear (Sierra Wireless)	AC340U
Netgear (Sierra Wireless)	AC341U
Novatel	MC760 3G
Novatel	MC990D
Novatel	MC996D
Novatel	U727
Novatel	U760
Novatel Wireless	MC545
Novatel Wireless	Merlin XU950D
Novatel Wireless	Ovation 930D
Novatel Wireless	Ovation MC950D HSUPA
Novatel Wireless	Ovation USB551L
Novatel Wireless	U679 Turbo Stick
Olivetti	Olicard 100
Olivetti	Olicard 145
Onda	MT503HS

Vendor	Model
Onda	MT505UP
Onda	MT8205 LTE
Onda	MW833UP
Onda	MW836UP-K
Onda	TM201
Onda	WM301
Option	Beemo
Option	GI0643
Option	Globetrotter
Option	GlobeTrotter GI1515
Option	iCon 461
Option	iCon 711
Pantech	P4200 LTE
Pantech	UML290
Pantech	UML295
Pantech / UTStarcom	UMW190
Samsung	GT-B1110
Samsung	GT-B3730
Samsung	SGH-Z810
Samsung	U209
Sierra Wireless	313, 320U
Sierra Wireless	AirCard 880U
Sierra Wireless	AirCard 881U
Sierra Wireless	Compass 597

Vendor	Model
Solomon	S3Gm-660
Sony Ericsson	MD300
Sony Ericsson	MD400
Sony Ericsson	MD400G
SpeedUp	SU-8000U
Toshiba	G450
TP-Link	MA180
TP-Link	MA260
UTStarcom	UM175
UTStarcom	UM185E
ZTE	6535-Z
ZTE	A371B
ZTE	AC2710
ZTE	AC2726
ZTE	AC581
ZTE	AC682
ZTE	AC8710
ZTE	AX226 WiMax
ZTE	K3520-Z
ZTE	K3565
ZTE	K3805-Z
ZTE	MF100
ZTE	MF110
ZTE	MF112

Vendor	Model
ZTE	MF190
ZTE	MF190J
ZTE	MF192
ZTE	MF196
ZTE	MF620
ZTE	MF622
ZTE	MF626
ZTE	MF628
ZTE	MF652
ZTE	MF656A
ZTE	MF668A
ZTE	MF669
ZTE	MF671
ZTE	MF680
ZTE	MF691 (T-Mobile Rocket 2.0)
ZTE	MF820 4G LTE
ZTE	MF821
ZTE	MF821D
ZTE	MU351

CHANGE LOG

May 21, 2015	Updated release for Supported FortiExtender Modems list v1.036.
October 29, 2014	Updated to include FortiGate supported modems.
September 5, 2014	Initial release.

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.